Safeguard Computer Security Evaluation Matrix (SCSEM)

Windows

2000, 2003, and NT

Release IV

10-Dec-07

Tester: *Insert Tester Name*
Date: *Insert Date(s) Testing Occured*
Location: *Insert Location testing was conducted*
Agency POC(s): *Insert Agency interviewee(s) names*

Test ID	NIST ID (800-53/A)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments/ Supporting Evidence
1	CM-6, AC-3, AU-9	Event Log Permissions	Look at the file permissions for: C:\%WINDIR%\system32\config\AppEvent.evt C:\%WINDIR%\system32\config\SecEvent.evt C:\%WINDIR%\system32\config\SysEvent.evt	Administrators (RX), Auditors (FULL) and System (FULL).			
2	AU-2, AU-3, CM-6	File Auditing Configuration	1. Check all NTFS volumes for file auditing. 2. Ensure that the "Everyone Group" is set to "FULL CONTROL" on the auditing tab.	Ensure that auditing is enabled for the Everyone group.			
3	AU-2, AU-3, AC-3	Local volumes are not formatted using NTFS.	1. Check all volumes on the system for file type by looking at My Computer. 2. Ensure all volumes are formatted with the NTFS file system.	All volumes are formatted with the NTFS file system.			
4	AC-3, CM-6	Disabled Service Permissions	1. Expand the “Security Configuration and Analysis” object in the tree window. 2. Expand the “System Services” object and select each applicable disabled Service. (Disabled Services can be identified using the Control Panel’s Services applet. 3. Right click the Service and select Security. 4. Select ‘View Security’ 5. If the ACLs for applicable disabled Services dMUST restrict permissions to Administrators, ‘full Control’, System ‘full control’, and Authenticated Users ‘Read’.	Service ACLs of disabled services is set to Administrators (Full Control), Authenticated Users (Read), and System (Full Control)			
5	CM-6, AC-3	File Share Permissions	1. Expand the “System Tools” object in the Tree window. 2. Select the “Shared Folders” object. 3. Select the “Shares” object. 4. Right click any user-created shares (ignore administrative shares; they usually have a “$” as the last character). 5. Select Properties. 6. Select the Share Permissions tab. 7. User-created file shares MUST BE reconfigured to remove ACL permissions from the “Everyone group”.	No Shares found that allow Everyone to connect.			
6	AC-2, CM-6	User account is dormant.	1. For all users on the system, perform the next steps. 2. From the command line type "net user username". 3. Ensure the Last Logon Date is not greater than 34 days.	All accounts have been logged in to within the past 34 days.			

7	AC-2, CM-6	A regular user has Administrator rights on the system.	1. From the command line, type "net localgroup administrators". 2. Ensure all users are valid and supposed to be part of the Administrators group.	All accounts listed in the Administrators group are valid and are supposed to be assigned to the Administratos group.			
8	AU-11	Security Event Preservation	1. Check the event viewer logs and ensure that the "application", "security", and "system" logs are set to save for no fewer than 14 days.	Event viewer logs are set to store for no fewer than 14 days.			
9	AU-11	Audit Storage Capacity	1. Click on "start" 2. Click "settings", then "control panel" 3. Click "administrative tools" 4. Click "event viewer" 5. Right-click "application, etc." 6. Right-click "properties". 7. Ensure that the minimum log size is as follows: The value for “Maximum application log size” MUST BE set to a minimum of “16384 kilobytes." The value for “Maximum security log size” MUST BE set to a minimum of “81920 kilobytes.” The value for “Maximum system log size” MUST BE set to a minimum of “16384 kilobytes.".	The minimum log size should reflect the following specs in "event viewer": The value for “Maximum application log size” MUST BE set to a minimum of “16384 kilobytes.". The value for “Maximum security log size” MUST BE set to a minimum of “81920 kilobytes." The value for “Maximum system log size” MUST BE set to a minimum of “16384 kilobytes."			
10	AC-5, AC-6, CM-6	An anonymous FTP connection within the enclave is permitted.	1. Go to the command prompt 2. Type ftp 127.0.0.1 3. Login to an ftp session using an authenticated user account. 4. The command response MUST NOT indicate that an anonymous FTP login was permitted. 5. Accounts with administrator privileges MUST NOT be used to access FTP.	Anonymous FTP is disabled and the anonymous user would not be granted administrative access.			
11	AC-11	Current user configuration is not set with a password-protected screen saver.	1. Right-click destop 2. Click properties 3. Click screen saver tab 4. Look to see that there is a password-protected screensaver set and that it is enabled to activate sooner that 15 minutes.	Ensure that a password-protected screensaver is set and that is activated sooner than 15 following inactivity.			

12	CM-6, IA-1, IA-2, IA-4	Account Password Expiration	1. Open Computer Management 2. Check user accounts to see if passwords expire on the system.	Passwords are required to expire for all user accounts. The following accounts are exempt from this check: : Built-in administrator accounts :Application accounts			
13	CM-6, AC-5, AC-6	Launching Windows Messenger	The following registry value must exist or its value set to 1: Registry Hive: HKEY_LOCAL_MACHINE Subkey: \Software\Policies\Microsoft\Messenger\Client Value Name: PreventRun	The user is not allowed to launch Windows Messenger (MSN Messenger, .NET Messenger)			
14	AC-17, MA-4	NetMeeting Remote Desktop Sharing	Check for encryption is being used when remotely accessing Windows. The following registry key must exist and its value is set to 1: Registry Hive: HKEY_LOCAL_MACHINE Subkey: \Software\Policies\Microsoft\Conferencing Value Name: NoRDS	Ensure that the value for the following registry key exists and that is set to 1: HKEY_LOCAL_MACHINE Subkey: \Software\Policies\Microsoft\Conferencing\ Value Name: NoRDS			
15	CM-6, AC-7, AC-10, AC-9	Terminal Services Logon Prompt	The following registry key does exist and its value is set to 1: Registry Hive: HKEY_LOCAL_MACHINE Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services Value Name: fPromptForPassword	Clients are always prompted for a password on connection			

16	CM-6, SC-4	Terminal Services Temporary Folder Creation	The following registry key does exist and its value is set to 1: Registry Hive: HKEY_LOCAL_MACHINE Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services Value Name: PerSessionTempDir	A common temporary folder is not used instead of a per-session temporary folder.			
17	CM-6, SC-4	Terminal Services Temp Folder Deletion	The following registry key does exist and its value is set to 1: Registry Hive: HKEY_LOCAL_MACHINE Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services Value Name: DeleteTempDirsOnExit	The temp folder is deleted when the session terminates.			
18	CM-6, AC-11	Screen Saver Default Lock	Tthe value for “MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)” is set to “0”.	The Screen saver grace period is set to 0.			
19	CM-6, AC-5, AC-6	Windows Messenger Internet Access	The following registry key does exist and its value is set to 1: Registry Hive: HKEY_LOCAL_MACHINE Subkey: \Software\Policies\Microsoft\Messenger\Client\{9b017612-c9f1-11d2-8d9f-0000f875c541}	Window messenger should be disabled in the following registry key: HKEY_LOCAL_MACHINE Subkey: \Software\Policies\Microsoft\Messenger\Client\{9b017612-c9f1-11d2-8d9f-0000f875c541}			
20	CM-6, AC-5, AC-6	DCOM Call Execution	1. Open the registry editor. 2. Go to HKLM\Software\Classes\Appid 3. Inspect all keys to ensure there are no RunAS registry keys. 4. No registry key has the RunAs enabled.	No RunAS Registry keys were found.			

21	CM-6, AU-2, AU-3	Registry Auditing	1. From the command line, type REGEDT32. 2. Expand Hkey_Local_Machine. 3. For both the System and Software Registry Keys, Right click System or Software and select Permissions. 4. Click the advanced button then select the Auditing tab. 5. Ensure the Everyone group is set to Full Control for auditing.	Audting is enabled on the HKLM\Software and HKLM\System registry keys.			
22	AC-3, CM-6	Anonymous Registry Access	1. From the command line, type REGEDT32. 2. Expand Hkey_Local_Machine/System/CurrentControlSet/Control/SecurePipeServers 3. Right click "Winreg" and select Permissions. 4. The security permission for Winreg is Administrators (Full Control, Backup operators (Read), and Local Service (Read).	Administrators (Full Control), Backup Operators (Read) and Local Serv ice (Read).			
23	AC-3	Object Ownership	1. Open the local security policy. 2. Move to Security Options. 3. The value for “System objects: Default owner for object created by members of the Administrators group” is set to “Object creator”.	The value for "System objects: Default owner for object created by members of the Administrators group" is set to "Object Creator".			
24	CM-6, SC-4	Virtual Memory Setting On Shutdown	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Shutdown: Clear virtual memory pagefile” is set to “Enabled”.	The value for “Shutdown: Clear virtual memory pagefile” is set to “Enabled”			

25	CM-6, AC-5, AC-6	Remotely Readable Removable Media	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Devices: Restrict floppy access to locally logged-on user only” is set to “Enabled”.	The value for “Devices: Restrict floppy access to locally logged-on user only” is set to “Enabled”.			
26	CM-6, AC-8	Legal Notice Logon Banner	1. Open the local security policy. 2. Move to Security Options. 3. The value for "Interactive Logon: Message text for users attempting to log on” includes information on Government Systems and consent to monitoring.	Legal notice contains warnings of consent to monitoring and identifies the system as a government system. "UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474, TITLE 18, UNITED STATES CODE. PUBLIC LAW 99-474 AND CHAPTER XXI, SECTION 1030 STATES THAT Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information, or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States, shall be punished by a fine under this title or imprisonment for not more than 10 years, or both. All activities on this system may be recorded and monitored. Individuals using this system expressly consent to such monitoring. Evidence of possible misconduct or abuse may be provided to appropriate officials. "			
27	CM-6, AU-9	Capturing Audit Events	1. Open the local security policy. 2. Move to Security Options. 3. The site has procedures in place and the value for “Audit: Shut down system immediately if unable to log security audits” is set to “Enabled”.	The value for “Audit: Shut down system immediately if unable to log security audits” is set to “Enabled”			

28	CM-6, AC-3	Share Access	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Network access: Do not allow anonymous enumeration of SAM accounts” is set to “Enabled”. 4. The value for “Network access: Do not allow anonymous enumeration of SAM accounts and shares” is set to “Enabled”.	The value for “Network access: Do not allow anonymous enumeration of SAM accounts” is set to “Enabled” The value for “Network access: Do not allow anonymous enumeration of SAM accounts and shares” is set to “Enabled”			
29	CM-6, AU-9	Event Log Access	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Prevent local guests group from accessing application log” is set to “Enabled”. 4. The value for “Prevent local guests group from accessing security log” is set to “Enabled”. 5. The value for “Prevent local guests group from accessing system log” is set to “Enabled”.	The value for “Prevent local guests group from accessing application log” is set to “Enabled” The value for “Prevent local guests group from accessing security log” is set to “Enabled” The value for “Prevent local guests group from accessing system log” is set to “Enabled”.			
30	IA-1, IA-2, IA-4	Password Complexity	1. Open the local security policy. 2. Move to Password Policy. 3. Ensure the Passwords must meet complexity requirements is set to "Enabled" (unless ENPASFLT.DLL is installed).	The value for "Passwords Must Meet Complexity Requiremtns" is set to Enabled. *Note - If the NSA ENPASFLT.DLL password filter is installed and activated, this option should be set to Disabled.			
31	CM-6, AC-5, AC-6	Print Driver Installation	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Devices: Prevent users from installing printer drivers” is set to “Enabled”.	The value for “Devices: Prevent users from installing printer drivers” is set to “Enabled”.			
32	CM-6, SC-4	Ctrl+Alt+Del Security	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Interactive Logon: Do not require CTRL ALT DEL” is set to “Disabled”.	The value for “Interactive Logon: Do not require CTRL ALT DEL” is set to “Disabled”.			
33	CM-6, SC-9, AC-18	Unencrypted SMB Passwords	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Microsoft Network Client: Send unencrypted password to connect to third-party SMB servers” is set to “Disabled”.	The value for “Microsoft Network Client: Send unencrypted password to connect to third-party SMB servers” is set to “Disabled”.			

34	CM-6, SC-9, AC-18	Outgoing Secure Channel Traffic Signing	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Domain Member: Digitally sign secure channel data (when possible)” is set to “Enabled”. 4. The value for “Secure channel: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”.	The value for “ Domain Member: Digitally sign secure channel data (when possible)” is set to “Enabled”. -or- “Secure channel: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”.			
35	CM-6, SC-9, AC-18	Outgoing Secure Channel Traffic Encryption	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Domain Member: Digitally encrypt secure channel data (when possible)” is set to “Enabled”. 4. The value for “Domain Member: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”.	The value for “Domain Member: Digitally encrypt secure channel data (when possible)” is set to “Enabled”. -or- “Domain Member: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”.			
36	CM-6, IA-1, IA-2, IA-4	The computer account password is prevented from being reset.	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Domain Member: Disable Machine Account Password Changes” is set to “Disabled”.	The value for ""Domain Member: Disable Machine Account Password Changes” is set to “Disabled”.			
37	CM-6, AC-5, AC-6	Permissions For Ejection Of Removable NTFS Media	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Devices: Allowed to Format and Eject Removable Media” is set to ” Administrators”.	The value for “Devices: Allowed to Format and Eject Removable Media” is set to ” Administrators”.			
38	CM-6, IA-1, IA-2, IA-4	Password Expiration Warning	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Interactive Logon: Prompt user to change password before expiration” is set to “14 days” or more.	The value for “Interactive Logon: Prompt user to change password before expiration” is set to “14 days” or more.			
39	AC-3	The default permissions of global system objects are not increased.	1. Open the local security policy. 2. Move to Security Options. 3. The value for “System Objects: Strengthen default permissions of internal system objects (e.g. Symbolic links)” is set to “Enabled”.	The value fo “System Objects: Strengthen default permissions of internal system objects (e.g. Symbolic links)” is set to “Enabled”.			

40	IA-1, IA-2, IA-4	Reversible Password Encryption	1. Open the local security policy. 2. Move to Password Policy. 3. The value for “Store password using reversible encryption for all users in the domain” is disabled.	The value for “Store password using reversible encryption for all users in the domain” is disabled.			
41	CM-6, AC-5, AC-6	The Server Operators group can schedule tasks.	1. If the system is not a Domain Controller, this is OK. 2. Open the local security policy. 3. Move to Security Options. 4. The value for “Domain Controller: Allow server operators to schedule tasks” is set to “Disabled”.	The Server Operators group cannot schedule tasks.			
42	AC-3, CM-6	Anonymous SID	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Network access: Allow anonymous SID/Name translation” is set to “Disabled”.	The value for “Network access: Allow anonymous SID/Name translation” is set to “Disabled”			
43	AC-3, CM-6	Named Pipes	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Network access: Named pipes that can be accessed anonymously” DOES NOT contains entries besides “COMNAP, COMNODE, SQL\QUERY, SPOOLSS, LLSRPC, browser.'	The value for “Network access: Named pipes that can be accessed anonymously” only contains “COMNAP, COMNODE, SQL\QUERY, SPOOLSS, LLSRPC, browser”.			
44	CM-6, AC-3	Unauthorized registry paths are remotely accessible.	1. Open the local security policy. 2. Move to Security Options. 3. • The value for “Network access: Remotely accessible registry paths” contains NO entries besides the following: System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Control\Server Applications System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\Userconfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration	The value for “Network access: Remotely accessible registry paths" contains only the entries listed in the Test Steps.			
45	CM-6, AC-3	Share Access	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Network access: Shares that can be accessed anonymously” includes NO entries.	The value for “Network access: Shares that can be accessed anonymously” does not include any entries.			

46	CM-6, AC-17, MA-4	Terminal Services Remote Control	1. The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Terminal Services “Sets rules for remote control of Terminal Services user settings” will be set to “Enabled” and the “Options” will be set to “No remote control allowed”.	Ensure the value for Computer Configuration -> Administrative Templates -> Windows Components -> Terminal Services “Sets rules for remote control of Terminal Services user settings” is set to “Enabled” and the “Options” is set to “No remote control allowed”.			
47	CM-6, AC-17, MA-4	Solicited Remote Assistance	1. The policy value for Computer Configuration -> Administrative Templates -> System -> Remote Assistance “Solicited Remote Assistance” will be set to “Disabled”.	The value for Computer Configuration -> Administrative Templates -> System -> Remote Assistance “Solicited Remote Assistance” is set to “Disabled”.			
48	AC-5, AC-6, CM-6	Everyone permissions are applied to anonymous users.	1. Open the local security policy. 2. Move to Security Options. 3.The value for “Network access: Let everyone permissions apply to anonymous users” is set to “Disabled."	The value for “Network access: Let everyone permissions apply to anonymous users” is set to “Disabled”.			
49	CM-6, SC-9, AC-18	NT LAN Manager (NTLM) Authentication	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Network security: Minimum session security for NTLM SSP based (including secure RPC) clients” is set to “Require NTLMv2 session security”, ”Require 128-bit encryption”, ”Require Message Integrity”, and ”Require Message Confidentiality.". 4. Microsoft warns that setting the value to "Require NTLMv2 session security” will prevent authentication, if the “Network security: LAN Manager authentication level” is set to permit NTLM or LM authentication."	The value for “Network security: Minimum session security for NTLM SSP based (including secure RPC) clients” is set to “Require NTLMv2 session security”, ”Require 128-bit encryption”, ”Require Message Integrity”, or ”Require Message Confidentiality”.			
50	CM-6, AC-17, MA-4	Remote Assistance Offers	1. The policy value for Computer Configuration -> Administrative Templates -> System -> Remote Assistance “Offer Remote Assistance” will be set to “Disabled”.	The value for Computer Configuration -> Administrative Templates -> System -> Remote Assistance “Offer Remote Assistance” is set to “Disabled”.			

51	CM-6, AC-3	Share Permissions	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Network access: Do not allow anonymous enumeration of SAM accounts” is set to “Enabled." 4. The value for “Network access: Do not allow anonymous enumeration of SAM accounts and shares” is set to “Enabled."	The value for “Network access: Do not allow anonymous enumeration of SAM accounts” is set to “Enabled” The value for “Network access: Do not allow anonymous enumeration of SAM accounts and shares” is set to “Enabled”			
52	CM-6, SC-9, AC-18	NTLM SSP-Based Server Encryption	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Network security: Minimum session security for NTLM SSP based (including secure RPC) servers” is set to “Require NTLMv2 session security”, ”Require 128-bit encryption”, ”Require Message Integrity”, and ”Require Message Confidentiality.". 4. Microsoft Warns “Require NTLMv2 session security” will prevent authentication, if the “Network security: LAN Manager authentication level” is set to permit NTLM or LM authentication.	The value for “Network security: Minimum session security for NTLM SSP based (including secure RPC) servers” is set to “Require NTLMv2 session security”, ”Require 128-bit encryption”, ”Require Message Integrity”, or ”Require Message Confidentiality”.			
53	CM-6, AC-13	Audit Event Threshold	1. Open the local security policy. 2. Move to Security Options. 3. The value for “MSS: (Warning Level) Percentage threshold for the security event log at which the system will generate a warning” is set to “90” or more.	The value for “MSS: (Warning Level) Percentage threshold for the security event log at which the system will generate a warning” is set to “90” or less.			
54	CM-6, IA-1, IA-2, IA-4	The computer account password is prevented from being reset.	1. If the system is not a Domain Controller this is OK. 2. Open the local security policy. 3. Move to Security Options. 4.The value for “Domain Controller: Refuse machine account password changes” is set to “Disabled."	The computer account password is not prevented from being reset.			
55	CM-6, SC-9, AC-18	Outgoing Secure Channel Traffic	1. Open the local security policy. 2. Move to Security Options. 3. Ensure the machine is part of a domain or this is N/A. 4. The value for “Domain Member: Digitally encrypt or sign secure channel data (always)” is set to “Enabled." 5. Microsoft Warns that enabling this setting will prevent a Windows XP system from authenticating properly with a Windows NT PDC/BDC.	The value for “Domain Member: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”.			
56	AC-3, CM-6	Named Pipes and Shares can be accessed anonymously.	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Network access: Restrict anonymous access to Named Pipes and Shares” is set to “Enabled."	Named Pipes and Shares cannot be accessed anonymously.			
57	AC-7, AC-9, AC-10	Failed Login Minimum Requirement	1. Open the local security policy. 2. Move to the Account Lockout Policy. 3.The “Account lockout threshold” is NOT “0” or more than three attempts.	The value for If the “Account lockout threshold” is “1” or less than or equal to three attempts.			

58	AC-7, AC-9, AC-10	Lockout Duration Minimum Requirement	1. Open the local security policy. 2. Move to the Account Lockout Policy. 3. The “Account lockout duration” is more than 60 minutes.	The value for “Account lockout duration” is more than or equal to 60 minutes.			
59	AC-5, AC-6	Unauthorized users are granted the right to â€œAct as part of the operating system.	1. Open thye local security policy. 2. Move to the User Rights Assignment. 3. No user accounts, or groups, (to include administrators) are granted the "Act as part of the operating system" righ.	Ensure no users are part of the "Act as part of the operating system" right assignment.			
60	AC-5, AC-6	User Rights Configuation	1. Open thye local security policy. 2. Move to the User Rights Assignment. 3. Ensure the following User Rights Assignments are assigned. 4. Refer to win2003_appendix	Ensure the User Rights Assignments follow what is in the test steps. Refer to Appendix B for more information.			
61	IA-1, IA-2, IA-4	Maximum password age does not meet minimum requirements.	1. Open the local security policy. 2. Move to Password Policy. 3. The value for the “Maximum password age”, is less than 60 daysfor privileged users, 90 days for non-privileged users. The value is NOT set to 0 (never expires).	While the NASA 2810 states that "passwords shall be changed at least annually", it is security industry best practice to enforce a policy of a password change every 90 days.			
62	IA-1, IA-2, IA-4	Minimum Password Age	1. Open the local security policy. 2. Move to Password Policy. 3. The value for the “Minimum password age”, is more than one day.	The value for “Minimum password age”, is more than or equal to one day.			

63	IA-1, IA-2, IA-4	Password History	1. Open the local security policy. 2. Move to Password Policy. 3. The value for “Enforce password history” is lmore than 5 passwords.	The value for “Enforce password history” is more than or equal to 6 passwords.			
64	AC-2, CM-6	The built-in guest account is not disabled.	1. Open the local security policy. 2. Move to Security Options. 3. IThe value for “Accounts: Guest account status” is set to ” Disabled."	The value for “Accounts: Guest account status” is set to ” Disabled”.			
65	CM-6, AC-2	Renaming Built-In Administrator Account	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Accounts: Rename guest account” is set to a value other than “Guest."	The value for “Accounts: Rename guest account” is set to a value other than “Guest”.			
66	AC-5, AC-6	Guests group is not assigned the right. Deny access this computer from the network.	1. Open thye local security policy. 2. Move to the User Rights Assignment. 3. The Guest group is assigned the right Deny access this computer from the network.	Ensure the guest group is assigned the user right Deny access this computer from the network.			
67	AC-18, SC-9	Kerberos user logon restrictions are not enforced.	1. Look at the local security policy. 2. Open the Kerberos Policy. 3. The “Enforce user logon restrictions” is set to "Enabled."	Kerberos user logon restrictions are enforced.			
68	AC-18, SC-9	Kerberos user ticket maximum lifetime does not meet minimum standards.	1. Look at the local security policy. 2. Open the Kerberos Policy. 3. The “Maximum lifetime for user ticket” is less than ‘10’ hours.	Kerberos user ticket maximum lifetime does meet minimum standards.			
69	AC-18, SC-9	Kerberos user ticket renewal maximum lifetime does not meet minimum standards.	1. Look at the local security policy. 2. Open the Kerberos Policy. 3. The “Maximum lifetime for user ticket renewal” is lessr than ‘7’ days.	Kerberos user ticket renewal maximum lifetime does meet minimum standards.			

70	AC-18, SC-9	Computer clock synchronization tolerance does not meet minimum standards.	1. Look at the local security policy. 2. Open the Kerberos Policy. 3. The “Maximum tolerance for computer clock synchronization” is less than ‘5’ minutes.	Computer clock synchronization tolerance does meet minimum standards.			
71	AC-5, AC-6	Terminal Services Logon Rights	1. Look at the local security policy. 2. Open User Rights Assignment. 3. Examine the User Right "Allow logon through Terminal Services". 4. No user accounts, or groups, (to include administrators) are granted this right.	Unauthorized users are not granted the right to “Allow logon through Terminal Services”.			
72	CM-6, IA-1, IA-2, IA-4	The maximum age for machine account passwords is not set to requirements.	1. Look at the local security policy. 2.Open Security Options. 3. The value for “Domain Member: Maximum Machine Account Password Age” is set to “30”, or less.	The maximum age for machine account passwords is set to requirements.			

73	AU-3, AU-2, AU-3	Auditing is not enabled.	1. Open Local Security Policy; 2. Open Audit Policy 3. Ensure that auditing is enabled for the policy fields. 01 The audit trail shall capture all successful login and logoff attempts. 02 The audit trail shall capture all unsuccessful login and authorization attempts. 03 The audit trail shall capture all identification and authentication attempts. 04 The audit trail shall capture all actions, connections and requests performed by privileged users (a user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users). 05 The audit trail shall capture all actions, connections and requests performed by privileged functions. 06 The audit trail shall capture all changes to logical access control authorities (e.g., rights, permissions). 07 The audit trail shall capture all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services. 08 The audit trail shall capture the creation, modification and deletion of objects including files, directories and user accounts. 09 The audit trail shall capture the creation, modification and deletion of user accounts and group accounts. 10 The audit trail shall capture the creation, modification and deletion of user account and group account privileges.	Auditing should be enabled for at least one of the policy fields in the auditing section of the Local Security Policy. 11 The audit trail shall capture: i) the date of the system event; ii) the time of the system event; iii) the type of system event initiated; and iv) the user account, system account, service or process responsible for initiating the system event. 12 The audit trail shall capture system startup and shutdown functions. 13 The audit trail shall capture modifications to administrator account(s) and administrator group account(s) including: i) escalation of user account privileges commensurate with administrator-equivalent account(s); and ii) adding or deleting users from the administrator group account(s). 14 The audit trail shall capture the enabling or disabling of audit report generation services. 15 The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, database). 16 The audit trail shall be protected from unauthorized access, use, deletion or modification. 17 The audit trail shall be restricted to personnel routinely responsible for performing security audit functions.			
74	AU-8	Audit trails are protected from modification, unauthorized access, and destruction.	C:\Windows\SYSTEM32\CONFIG directory → display its contents → view security permissions.	Security permissions for C:\Windows\SYSTEM32\CONFIG -Administrators, Auditors			

75	AU-8	Event logs are configured to be protected from guests.	Using the Microsoft Management Console tool, perform a basic Security Configuration and Analysis. Under the “Security Configuration” section, click “Event Log”, and select “Settings for Event Log”. Inspect the settings for reasonableness.	The event logs should be retained for a significant period of time and cleared manually. Retention should be controlled manually. The event logs should be completely restricted from guest accounts. The computer should shut down in the event of the logs becoming full. • Event logs are restricted from guest access: - HKLM\ System\ CurrentControlSet\ Services\ EventLog\ Application\ RestrictGuestAccess: REG_DWORD : 1 - HKLM\ System\ CurrentControlSet\ Services\ EventLog\ Security\ RestrictGuestAccess: REG_DWORD : 1 - HKLM\ System\ CurrentControlSet\ Services\ EventLog\ System\ RestrictGuestAccess: REG_DWORD : 1			
76	AU-4	Event logs are configured to be retained and protected in the event of becoming full.	Local security settings → Local Security Policies → Security Options → Verify Windows system “Shut Down system immediately if unable to log security alerts”	• "Shut Down system immediately if unable to log security alerts” : - Enabled			
77	IA-3	Password history is maintained for a minimum of six (6) generations.	Using the Local Security Policy tool, review the “Password Policy” section of the Account Policies and determine the computer setting for “Enforce password history”.	• Verify Password Policy “Enforce password history” is: - Six (6) passwords remembered			
78	IA-3	User accounts that are inactive for a period of 90 days are revoked. This includes new user accounts that have never been accessed.	Consult with the system administrator to verify procedures for identifying inactive accounts and blocking/deleting them.	The system administrator reviews the list of user accounts consistently to identify inactive accounts. The system administrator also reviews the list of new user accounts to identify ones that have never been activated.			
79	CM-6, IA-1, IA-2, IA-4	User account does not require a password.	1. Open Local Security Policy 2. Check to see if user accounts require a password.	User accounts require a the use of a password.			

80	IA-1, IA-2, IA-4,	Minimum Password Length	1. Open Local Security Policy 2. Ensure Password Length is set to 9 characters.	Password length must be between 8 and 128 characters.			
81	SC-2	The virtual memory pagefile is wiped clean when Windows shuts down.	Using the Local Security Policy tool, review the “Security Options” section of the Local Policies and determine the computer setting for “Clear virtual memory pagefile when system shuts down”.	• Windows 2003 Security Option “Shutdown: Clear Virtual Memory Pagefile” should be: Enabled			
82	SC-2	FTI files and folders, when deleted, are removed from the Recycle Bin immediately.	Select the Programs | Windows NT Explorer. Select Recycle Bin folder by clicking its icon. Click on File | Properties menu item within the Recycle Bin window.	The “Do not move files to the recycle bin. Remove files immediately on delete” is enabled.			
83	AC-4	Information flow enforcement Information	Computer Configuration -> Administrative Templates-> Windows Components -> Intern	Security ZonesL Use only machine settings will be set to enable HKEY-LOCAL-MACHINE Subkey: \Software\Policies\Microsoft\Windows\Current\Version\InternetSettings\ Value Name: Secuirty_HKLM-only Type: REG_DWORD Value: 1 The registry value does exist and equals one			
84	AC-12	Does system terminate terminal and remote sessions after a specific period of activity.	Computer Configuration-> Administrative Templates-> Windows Components -> Terminal Services-> Sessions	"Set time limit for active but idle Terminal Services sessions" set to ENABLED "Idle session limit" set to 15 minutes or less			
85	AC-14	Permitted Actions without Identification or Authorization Only actions necessary to accomplish a specific organizational objective may be conducted without Identification and Authorization	Check that windows is configured to prevent anonymous access to unauthorized network share	Network access: Shares that can be accessed anonymously must be empty			

86	AU-5	Response to Audit Processing Failures	Audit: Shut down system immediately if unable to log security audits This policy setting determines whether the computer shuts down immediately if it is unable to log security events. The amount of administrative overhead that was required to enable the Audit: Shut down system immediately if unable to log security audits setting in the LC and EC environments was determined to be too great. Therefore, this policy setting is configured to Disabled in the baseline policy for those environments. However, this policy setting is configured to Enabled in the baseline policy for the SSLF environment because the additional administrative overhead was deemed acceptable to prevent the deletion of events from the Security log unless an administrator specifically chooses to do so.	Setting Legacy Client Enterprise Client Specialized Security – Limited Functionality Audit the access of global system objects Disabled Disabled Disabled Audit the use of Backup and Restore privilege Disabled Disabled Disabled Shut down system immediately if unable to log security audits Disabled Disabled Enabled			
87	AC-5, AC-6	User Rights Configuation	1. Open the local security policy. 2. Move to the User Rights Assignment. 3. Ensure the following User Rights Assignments are assigned. 4. Refer to win2003_appendix.				
88	CM-7, SA-9	Unnecessary services are run on the system.	1. Look at the services running on the local machine and compare them to win2003_appendix. 2. Ensure that the appropriate services are disabled.				
89	CM-4	Vulnerable or unnecessary network services are not employed on the machine.	Logon to the Windows machine as an administrative user and execute the Services tool. Inspect the enabled network services for reasonableness. The following services should ideally be disabled: Remote Registry Service, Telnet, Alerter, Server, FTP, Messenger, and SNMP.	The following services should ideally be disabled: Remote Registry Service, Telnet, Alerter, Server, FTP, Messenger, and SNMP.			
90	CM-4	The system is formatted with the Windows NT file system (NTFS) for all partitions.	Using the Disk Manager tool, view the logical volumes.	The Disk Manager should show NTFS for all local file systems.			
91	CM-4	IP forwarding and IP source routing have been disabled.	Logon to the Windows machine as an administrative user and execute the Registry Editor. Locate the “HKEY_LOCAL_MACHINE | System | CurrentControlSet | Services | Tcpip | Parameters” folder and locate the “IPEnableRouter” key.	• Locate “HKEY_LOCAL_MACHINE | System | CurrentControlSet | Services | Tcpip | Parameters” verify key setting: Windows 2003 registry key			

92	CM-4	The system is free of irrelevant files and registry entries.	Using Windows Explorer, display the contents of the following directories: • C:\WINNT\system32\dllcache; C:\WINNT\system32\os2; C:\WINNT\system32 Additionally, execute the Registry Editor and locate the following keys: • HKLM\System\CurrentControlSet\Control \Session Manager\Environment\Os2LibPath • HKLM\System\CurrentControlSet\Control \Session Manager\Subsystems\Optional • HKLM\System\CurrentControlSet\Control \Session Manager\Subsystems\OS2 and • HKLM\System\CurrentControlSet\Control \Session Manager\Subsystems\ POSIX	• "C:\WINNT\system32\dllcache" should not contain: a. os2.exe, os2ss.exe, os2srv.exe, psxss.exe, posix.exe, and psxdll.dll • "C:\WINNT\system32\os2" should not contain: a. os2.exe, os2ss.exe, os2srv.exe, psxss.exe, posix.exe, and psxdll.dll b. The os2 directory should not contain any files or folders with the exception of a dll folder, which must be kept intact for system performance. • Os2LibPath, Optional, OS2, and POSIX registry keys should not exist.			
93	CM-3	The Windows operating system have multi-boot capability.	Double click on the "My Computer" icon on the Desktop. Double click the system partition and locate the boot.ini file. Double click the boot.ini file to open it with notepad. Additionally, using Windows Explorer, explore the root directory of C:\ and D:\.	• In boot.ini, under "[operating systems], only two lines should be listed: Multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows XP Professional" Multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows XP Professional [VGA mode]/basevideo/sos" • In the root directory of C:\ and D:\ only one instance of the directories \Windows, \WinNT32, and \WinNT should exist			
94	CM-3	The Task Scheduler and NT Messenger services are correctly configured.	Using the Microsoft Management Console tool, perform a basic Security Configuration and Analysis. Under the "Security Configuration" section, click System Services, and locate Messenger and NT Task Scheduler. Right click on both of these items, select "Security", select "View Security", and select "Advanced".	The following permissions should be set for Administrator and System: Administrators Query Configuration Query Status Enumerate dependents Stop Interrogate Read System Read Start Stop			
95	CM-3	The DirectDraw access to video hardware and memory is disabled.	Logon to the Windows machine as an administrative user and execute the Registry Editor. Navigate to HKLM | SYSTEM | CurrentControlSet | Control | GraphicsDrivers | DCI and observe the value for "Timeout" (REG_DWORD).	• Locate "HKLM | SYSTEM | CurrentControlSet | Control | GraphicsDrivers | DCI" and verify registry value for "Timeout" is set to zero "0".			
96	CM-6, AC-1, AC-3	File Permissions	1. Check the file permissions on the folders and files listed in win2003_appendix.				

NIST ID (800-53/A)	Test Objective	Test Steps / Expected Results			Pass /Fail	Actual Results	Comments/Supporting Evidence
AC-6	Proper permissions are established for system files and folders.	Procedures: Using the Local Security Policy tool, review the “User Rights Assignment” section of the Local Policies. Expected Results: • The user rights displayed are consistent with those listed in below for Windows 2003.					
		File/Folder Name	**User Groups**	**Permissions**			
		%SystemDrive%	Administrator	Full			
			System	Full			
			Creator Owner	Full			
			Interactive	Read, Execute			
		%SystemRoot%\system32\	Administrator	Full			
		at.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		attrib.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		cacls.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		debug.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		drwatson.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		drwtsn32.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		edlin.exe	System	Full			
			Interactive	Full			
		%SystemRoot%\system32\	Administrator	Full			
		eventcreate.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		eventtriggers.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		ftp.exe	System	Full			
			Interactive	Full			
		%SystemRoot%\system32\	Administrator	Full			
		net.exe	System	Full			
			Interactive	Full			
		%SystemRoot%\system32\	Administrator	Full			
		net1.exe	System	Full			
			Interactive	Full			
		File/Folder Name	**User Rights**	**Authorized User Groups**			
		%SystemRoot%\system32\	Administrator	Full			

		netsh.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		rcp.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		reg.exe	System	Full			
		%SystemRoot%\regedit.exe	Administrator	Full			
			System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		regedt32.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		regsvr32.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		rexec.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		rsh.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		runas.exe	System	Full			
			Interactive	Full			
		%SystemRoot%\system32\	Administrator	Full			
		sc.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		subst.exe	System	Full			
		%SystemRoot%\system32\	Administrator	Full			
		telnet.exe	System	Full			
			Interactive	Full			
		%SystemRoot%\system32\	Administrator	Full			
		tftp.exe	System	Full			
			Interactive	Full			
		%SystemRoot%\system32\	Administrator	Full			
		tlntsvr.exe	System	Full			
AC-2	Permissions for registry keys are set properly.	Procedures: Using the Local Security Policy tool, review the “User Rights Assignment” section of the Local Policies.					
		Registry Key	**User Groups**	**Permissions**			
		HKLM\Software	Administrators	Full			
			System	Full			
			Creator Owner	Full			
			Users	Read			
		HKLM\Software\Microsoft\	Administrators	Full			
		Windows\CurrentVersion\Installer	System	Full			
			Users	Read			
		HKLM\Software\Microsoft\	Administrators	Full			
		Windows\CurrentVersion\Policies	System	Full			
			Authenticated Users	Read			
		HKLM\System	Administrators	Full			
			System	Full			

			Creator Owner	Full			
			Users	Read			
		HKLM\System\	Administrators	Full			
		CurrentControlSet\Enum	System	Full			
			Authenticated Users	Read			
		HKLM\System\CurrentControl Set\ Services\SNMP\Parameters\	Administrators	Full			
		PermittedManagers	System	Full			
			Creator Owner	Full			
		HKLM\System\CurrentControl Set\ Services\SNMP\Parameters\	Administrators	Full			
		ValidCommunities	System	Full			
			Creator Owner	Full			
		Registry Key	**User Groups**	**Permissions**			
		HKLM\SOFTWARE\Microsoft\	Administrators	Full			
		Windows\CurrentVersion\Polici es\ Ratings	Users	Read			
		HKLM\Software\Microsoft\MS DTC	Administrators	Full			
			System	Full			
			Users	Read			
			Network Service	Query value, Set value, Create subkey, Enumerate Subkeys, Notify, Read permissions			
		HKU\.Default\Software\Micros oft\ SystemCertificates\Root\ ProtectedRoots	Administrators	Full			
			System	Full			
			Users	Read			
		HKLM \SOFTWARE\Microsoft\ Windows NT\CurrentVersion\ SeCEdit	Administrators	Full			
			System	Full			
			Users	Read			
AC-6	Only authorized users are able to perform administrative tasks that can affect system security. General user accounts do not have administrator privileges.	Procedures: Using the Local Security Policy tool, review the “User Rights Assignment” section of the Local Policies. Expected Results: • The user rights displayed are consistent with those listed in below for Windows 2003.					
		Policy	**Expected Settings**				
		Access this computer from the network	Administrators				

		Act as part of the operating system	No One				
		Add workstations to the domain	Not Defined				
		Adjust memory quotas for a process (2003)	Not Defined				
		Allow log on locally (2003)	Administrators				
		Allow log on through terminal services (2003)	Administrators				
		Backup files and directories	Administrators, Backup Operators				
		Bypass traverse checking	Authenticated Users				
		Change the system time	Administrators				
		Create a page-file	Administrators				
		Create a token object	No One				
		Create global objects (2003)	Not defined				
		Create permanent shared object	No One				
		Debug programs	No One				
		Deny access to this computer from the network	Anonymous logon, Guest				
		Deny logon as a batch job	No One				
		Deny logon as a service	No One				
		Deny logon locally	No One				
		Deny logon through terminal service (2003)	Not defined				
		Policy	**Expected Settings**				
		Enable computer and user accounts to be trusted for delegation	No One				
		Force shutdown from a remote system	Administrators				
		Generate Security Audits	Local Service, Network Service				
		Impersonate a client after authentication (2003)	Service				
		Increase quotas	Administrators				
		Increase scheduling priority	Administrators				
		Load and unload device drivers	Administrators				
		Lock pages in memory	No One				
		Log on as a batch job	No One				
		Log on as a service	As needed				
		Log on locally	Administrator, (other specific users)				
		Manage auditing and security log	Administrators				
		Modify firmware environment values	Administrators				
		Perform volume maintenance tasks (2003)	Administrators				

		Profile single process	Administrators				
		Profile system performance	Administrators				
		Remove computer from docking station	Administrators and Authenticated Users (for workstations)				
		Replace a process level token	Network Service, Local Service				
		Restore files and directories	Administrators, Backup Operators				
		Shut down the system	Administrators				
		Synchronize directory service data	No One				
		Take ownership of files or other objects	Administrators				

Test ID	NIST ID (800-53/A)	Test Objective	Test Steps	Expected Results	Actual Results	Pass/ Fail	Comments/ Supporting Evidence
1	AC-3, AU-9	Event Log Permissions	Look at the file permissions for: C:\%WINDIR%\system32\config\AppEvent.evt C:\%WINDIR%\system32\config\SecEvent.evt C:\%WINDIR%\system32\config\SysEvent.evt	Administrators (RX), Auditors (FULL) and System (FULL).			
2	AU-2, AU-3,	File Auditing Configuration	1. Check all NTFS volumes for file auditing. 2. Ensure that the "Everyone Group" is set to "FULL CONTROL" on the auditing tab.	Ensure that auditing is enabled for the Everyone group.			
3	AC-5, AC-6,	A Windows system has incorrect Default DCOM access permissions.	1. On the command line, execute Dcomcnfg.exe. 2. Select the Default Security tab. 3. Click the “Edit Default” button, and verify that only the Administrators and Interactive groups have the “allow access” permission. 4. Unauthorized accounts MUST NOT have the “allow access” permission.	The Windows system does not have incorrect Default DCOM access permissions.			
4	AU-2, AU-3, AC-3	Local volumes are not formatted using NTFS.	1. Check all volumes on the system for file type by looking at My Computer. 2. Ensure all volumes are formatted with the NTFS file system.	All volumes are formatted with the NTFS file system.			
5	AC-3,	Disabled Service Permissions	1. Expand the “Security Configuration and Analysis” object in the tree window. 2. Expand the “System Services” object and select each applicable disabled Service. (Disabled Services can be identified using the Control Panel’s Services applet. 3. Right click the Service and select Security. 4. Select ‘View Security’ 5. If the ACLs for applicable disabled Services dMUST restrict permissions to Administrators, ‘full Control’, System ‘full control’, and Authenticated Users ‘Read’.	Service ACLs of disabled services is set to Administrators (Full Control), Authenticated Users (Read), and System (Full Control)			
6	AC-5, AC-6	DCOM calls are not executed under the security context of the calling user.	1. Using the Registry Editor, go to the following Registry key: HKLM\Software\Classes\Appid 2. View each subkey in turn and verify that the RunAs value has not been added. 3. No subkey should have a RunAs value.	DCOM calls are executed under the security context of the calling user.			

7	AC-1, AC-3	File Share Permissions	1. Expand the “System Tools” object in the Tree window. 2. Select the “Shared Folders” object. 3. Select the “Shares” object. 4. Right click any user-created shares (ignore administrative shares; they usually have a “$” as the last character). 5. Select Properties. 6. Select the Share Permissions tab. 7. User-created file shares MUST BE reconfigured to remove ACL permissions from the “Everyone group”.	No Shares found that allow Everyone to connect.			
8	AC-2,	User account is dormant.	1. For all users on the system, perform the next steps. 2. From the command line type "net user username". 3. Ensure the Last Logon Date is not greater than 34 days.	All accounts have been logged in to within the past 34 days.			
9	AC-2,	A regular user has Administrator rights on the system.	1. From the command line, type "net localgroup administrators". 2. Ensure all users are valid and supposed to be part of the Administrators group.	All accounts listed in the Administrators group are valid and are supposed to be assigned to the Administratos group.			
10	AU-11, AU-1	Security Event Preservation	1. Check the event viewer logs and ensure that the "application", "security", and "system" logs are set to save for no fewer than 14 days.	Event viewer logs are set to store for no fewer than 14 days.			
11	AU-11, AU-1	Audit Storage Capacity	1. Click on "start" 2. Click "settings", then "control panel" 3. Click "administrative tools" 4. Click "event viewer" 5. Right-click "application, etc." 6. Right-click "properties". 7. Ensure that the minimum log size is as follows: The value for “Maximum application log size” MUST BE set to a minimum of “16384 kilobytes." The value for “Maximum security log size” MUST BE set to a minimum of “81920 kilobytes.” The value for “Maximum system log size” MUST BE set to a minimum of “16384 kilobytes.".	The minimum log size should reflect the following specs in "event viewer": The value for “Maximum application log size” MUST BE set to a minimum of “16384 kilobytes.". The value for “Maximum security log size” MUST BE set to a minimum of “81920 kilobytes." The value for “Maximum system log size” MUST BE set to a minimum of “16384 kilobytes."			

12	AC-5, AC-6,	An anonymous FTP connection within the enclave is permitted.	1. Go to the command prompt 2. Type ftp 127.0.0.1 3. Login to an ftp session using an authenticated user account. 4. The command response MUST NOT indicate that an anonymous FTP login was permitted. 5. Accounts with administrator privileges MUST NOT be used to access FTP.	Anonymous FTP is disabled and the anonymous user would not be granted administrative access.			
13	AC-11	Current user configuration is not set with a password-protected screen saver.	1. Right-click destop 2. Click properties 3. Click screen saver tab 4. Look to see that there is a password-protected screensaver set and that it is enabled to activate sooner that 15 minutes.	Ensure that a password-protected screensaver is set and that is activated sooner than 15 following inactivity.			
14	AC-17, MA-4	NetMeeting Remote Desktop Sharing	The following registry key must exist and its value is set to 1: Registry Hive: HKEY_LOCAL_MACHINE Subkey: \Software\Policies\Microsoft\Conferencing Value Name: NoRDS	Ensure that the value for the following registry key exists and that is set to 1: HKEY_LOCAL_MACHINE Subkey: \Software\Policies\Microsoft\Conferencing\ Value Name: NoRDS			
15	AC-2	Local users exist on a workstation in a domain.	1. From the command prompt, type Net user. 2. If the system is on a Domain, there should be no local user accounts besides the built-in Administrator, built-in Guest and decoy Administrator account. 3. If there are local user accounts on the system and the system is not on a domain, this is OK.	1. System on Domain: No local user accounts. 2. Sytstem not on Domain: Local user accounts are allowed.			
16	AC-5, AC-6	Windows Messenger Internet Access	The following registry key does exist and its value is set to 1: Registry Hive: HKEY_LOCAL_MACHINE Subkey: \Software\Policies\Microsoft\Messenger\Client\{9b017612-c9f1-11d2-8d9f-0000f875c541}	Window messenger should be disabled in the following registry key: HKEY_LOCAL_MACHINE Subkey: \Software\Policies\Microsoft\Messenger\Client\{9b017612-c9f1-11d2-8d9f-0000f875c541}			
17	AU-2, AU-3	Registry Auditing	1. From the command line, type REGEDT32. 2. Expand Hkey_Local_Machine. 3. For both the System and Software Registry Keys, Right click System or Software and select Permissions. 4. Click the advanced button then select the Auditing tab. 5. Ensure the Everyone group is set to Full Control for auditing.	Audting is enabled on the HKLM\Software and HKLM\System registry keys.			

18	AC-3	Anonymous Registry Access	1. From the command line, type REGEDT32. 2. Expand Hkey_Local_Machine/System/CurrentControlSet/Control/SecurePipeServers 3. Right click "Winreg" and select Permissions. 4. The security permission for Winreg is Administrators (Full Control, Backup operators (Read), and Local Service (Read).	Administrators (Full Control), Backup Operators (Read) and Local Serv ice (Read).			
19	, AC-8	Legal Notice Logon Banner	1. Open the local security policy. 2. Move to Security Options. 3. The value for "Interactive Logon: Message text for users attempting to log on" includes information on Government Systems and consent to monitoring.	Legal notice contains warnings of consent to monitoring and identifies the system as a government system. "UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474, TITLE 18, UNITED STATES CODE. PUBLIC LAW 99-474 AND CHAPTER XXI, SECTION 1030 STATES THAT Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information, or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States, shall be punished by a fine under this title or imprisonment for not more than 10 years, or both. All activities on this system may be recorded and monitored. Individuals using this system expressly consent to such monitoring. Evidence of possible misconduct or abuse may be provided to appropriate officials. "			
20	AU-9	Capturing Audit Events	1. Open the local security policy. 2. Move to Security Options. 3. The site has procedures in place and the value for "Audit: Shut down system immediately if unable to log security audits" is set to "Enabled".	The value for "Audit: Shut down system immediately if unable to log security audits" is set to "Enabled"			

21	AU-9	Event Log Access	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Prevent local guests group from accessing application log” is set to “Enabled”. 4. The value for “Prevent local guests group from accessing security log” is set to “Enabled”. 5. The value for “Prevent local guests group from accessing system log” is set to “Enabled”.	The value for “Prevent local guests group from accessing application log” is set to “Enabled” The value for “Prevent local guests group from accessing security log” is set to “Enabled” The value for “Prevent local guests group from accessing system log” is set to “Enabled”.			
22	SC-9	Outgoing Secure Channel Traffic Signing	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Domain Member: Digitally sign secure channel data (when possible)” is set to “Enabled”. 4. The value for “Secure channel: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”.	The value for “ Domain Member: Digitally sign secure channel data (when possible)” is set to “Enabled”. -or- “Secure channel: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”.			
23	SC-9	Outgoing Secure Channel Traffic Encryption	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Domain Member: Digitally encrypt secure channel data (when possible)” is set to “Enabled”. 4. The value for “Domain Member: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”.	The value for “Domain Member: Digitally encrypt secure channel data (when possible)” is set to “Enabled”. -or- “Domain Member: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”.			
24	IA-1, IA-2, IA-4	The computer account password is prevented from being reset.	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Domain Member: Disable Machine Account Password Changes” is set to “Disabled”.	The value for ""Domain Member: Disable Machine Account Password Changes” is set to “Disabled”.			
25	AC-5, AC-6	Permissions For Ejection Of Removable NTFS Media	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Devices: Allowed to Format and Eject Removable Media” is set to ” Administrators”.	The value for “Devices: Allowed to Format and Eject Removable Media” is set to ” Administrators”.			
26	IA-1, IA-2, IA-4	Password Expiration Warning	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Interactive Logon: Prompt user to change password before expiration” is set to “14 days” or more.	The value for “Interactive Logon: Prompt user to change password before expiration” is set to “14 days” or more.			
27	AC-3	The default permissions of global system objects are not increased.	1. Open the local security policy. 2. Move to Security Options. 3. The value for “System Objects: Strengthen default permissions of internal system objects (e.g. Symbolic links)” is set to “Enabled”.	The value fo “System Objects: Strengthen default permissions of internal system objects (e.g. Symbolic links)” is set to “Enabled”.			

28	IA-1, IA-2, IA-4	Reversible Password Encryption	1. Open the local security policy. 2. Move to Password Policy. 3. The value for “Store password using reversible encryption for all users in the domain” is disabled.	The value for “Store password using reversible encryption for all users in the domain” is disabled.			
29	, AC-5, AC-6	The Server Operators group can schedule tasks.	1. If the system is not a Domain Controller, this is OK. 2. Open the local security policy. 3. Move to Security Options. 4. The value for “Domain Controller: Allow server operators to schedule tasks” is set to “Disabled”.	The Server Operators group cannot schedule tasks.			
30	AC-3,	Anonymous SID	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Network access: Allow anonymous SID/Name translation” is set to “Disabled”.	The value for “Network access: Allow anonymous SID/Name translation” is set to “Disabled”			
31	SC-9, AC-18	NT LAN Manager (NTLM) Authentication	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Network security: Minimum session security for NTLM SSP based (including secure RPC) clients” is set to “Require NTLMv2 session security”, ”Require 128-bit encryption”, ”Require Message Integrity”, and ”Require Message Confidentiality.". 4. Microsoft warns that setting the value to "Require NTLMv2 session security” will prevent authentication, if the “Network security: LAN Manager authentication level” is set to permit NTLM or LM authentication."	The value for “Network security: Minimum session security for NTLM SSP based (including secure RPC) clients” is set to “Require NTLMv2 session security”, ”Require 128-bit encryption”, ”Require Message Integrity”, or ”Require Message Confidentiality”.			
32	, AC-3	Share Permissions	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Network access: Do not allow anonymous enumeration of SAM accounts” is set to “Enabled." 4. The value for “Network access: Do not allow anonymous enumeration of SAM accounts and shares” is set to “Enabled."	The value for “Network access: Do not allow anonymous enumeration of SAM accounts” is set to “Enabled” The value for “Network access: Do not allow anonymous enumeration of SAM accounts and shares” is set to “Enabled”			

33	, AC-13	Audit Event Threshold	1. Open the local security policy. 2. Move to Security Options. 3. The value for “MSS: (Warning Level) Percentage threshold for the security event log at which the system will generate a warning” is set to “90” or more.	The value for “MSS: (Warning Level) Percentage threshold for the security event log at which the system will generate a warning” is set to “90” or less.			
34	AC-7, AC-9, AC-10	Failed Login Minimum Requirement	1. Open the local security policy. 2. Move to the Account Lockout Policy. 3.The “Account lockout threshold” is NOT “0” or more than three attempts.	The value for If the “Account lockout threshold” is “1” or less than or equal to three attempts.			
35	AC-7, AC-9, AC-10	Failed Login Counter reset Time	1. Open the local security policy. 2. Move to the Account Lockout Policy. 3. The “Reset account lockout counter after” value is more than 60 minutes.	The value for “Reset account lockout counter after” value is more than or equal to 60 minutes.			
36	AC-5, AC-6	Unauthorized users are granted the right to â€œAct as part of the operating system.	1. Open thye local security policy. 2. Move to the User Rights Assignment. 3. No user accounts, or groups, (to include administrators) are granted the "Act as part of the operating system" righ.	Ensure no users are part of the "Act as part of the operating system" right assignment.			
37	AC-5, AC-6	User Rights Configuation	1. Open the local security policy. 2. Move to the User Rights Assignment. 3. Ensure the following User Rights Assignments are assigned. 4. Refer to win2000_appendix.	Ensure the User Rights Assignments follow what is in the test steps. Refer to win2000_appendix for more information.			

38	IA-1, IA-2, IA-4	Maximum password age does not meet minimum requirements.	1. Open the local security policy. 2. Move to Password Policy. 3. The value for the “Maximum password age”, is less than 60 days for privileged users, 90 days for non-privileged users. The value is NOT set to 0 (never expires).	While the NASA 2810 states that "passwords shall be changed at least annually", it is security industry best practice to enforce a policy of a password change every 90 days.			
39	IA-1, IA-2, IA-4	Minimum Password Age	1. Open the local security policy. 2. Move to Password Policy. 3. The value for the “Minimum password age”, is more than one day.	The value for “Minimum password age”, is more than or equal to one day.			
40	IA-1, IA-2, IA-4	Password History	1. Open the local security policy. 2. Move to Password Policy. 3. The value for “Enforce password history” is lmore than 5 passwords.	The value for “Enforce password history” is more than or equal to 5 passwords.			
41	AC-2,	The built-in guest account is not disabled.	1. Open the local security policy. 2. Move to Security Options. 3. IThe value for “Accounts: Guest account status” is set to ” Disabled."	The value for “Accounts: Guest account status” is set to ” Disabled”.			
42	, AC-2	Renaming Built-In Administrator Account	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Accounts: Rename guest account” is set to a value other than “Guest."	The value for “Accounts: Rename guest account” is set to a value other than “Guest”.			
43	, AC-2	The built-in administrator account has not been renamed.	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Accounts: Rename administrator account” is set to a value other than “Administrator."	The value for “Accounts: Rename administrator account” is set to a value other than “Administrator”.			
44	AC-5, AC-6	Guests group is not assigned the right. Deny access this computer from the network.	1. Open thye local security policy. 2. Move to the User Rights Assignment. 3. The Guest group is assigned the right Deny access this computer from the network.	Ensure the guest group is assigned the user right Deny access this computer from the network.			
45	AC-5, AC-6	Guests Group Local Logon Permissions	1. Open thye local security policy. 2. Move to the User Rights Assignment. 3. The Guest group is assigned the right Deny log on locally.	Ensure the guest group is assigned the user right Deny log on locally.			
46	AC-18, SC-9	Kerberos user logon restrictions are not enforced.	1. Look at the local security policy. 2. Open the Kerberos Policy. 3. The “Enforce user logon restrictions” is set to ‘Enabled."	Kerberos user logon restrictions are enforced.			

47	AC-18, SC-9	Kerberos user ticket renewal maximum lifetime does not meet minimum standards.	1. Look at the local security policy. 2. Open the Kerberos Policy. 3. The “Maximum lifetime for user ticket renewal” is lessr than ‘7’ days.	Kerberos user ticket renewal maximum lifetime does meet minimum standards.			
48	AC-18, SC-9	Computer clock synchronization tolerance does not meet minimum standards.	1. Look at the local security policy. 2. Open the Kerberos Policy. 3. The “Maximum tolerance for computer clock synchronization” is less than ‘5’ minutes.	Computer clock synchronization tolerance does meet minimum standards.			
49	AU-3, AU-2, AU-3	System-auditing configuration does not meet minimum requirements.	1. Open Local Security Policy; 2. Open Audit Policy; 3. Ensure that the system audits: 01 The audit trail shall capture all successful login and logoff attempts. 02 The audit trail shall capture all unsuccessful login and authorization attempts. 03 The audit trail shall capture all identification and authentication attempts. 04 The audit trail shall capture all actions, connections and requests performed by privileged users (a user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users). 05 The audit trail shall capture all actions, connections and requests performed by privileged functions. 06 The audit trail shall capture all changes to logical access control authorities (e.g., rights, permissions). 07 The audit trail shall capture all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services. 08 The audit trail shall capture the creation, modification/deletion of objects (files, directories) 09 The audit trail shall capture the creation, modification/deletion of user and group accounts. (continued in next column)	Auditing should be enabled in the Auditing section of the Local Security Policy. Events (cont.) 10 The audit trail shall capture the creation, modification and deletion of user account and group account privileges. 11 The audit trail shall capture: i) the date of the system event; ii) the time of the system event; iii) the type of system event initiated; and iv) the user account, system account, service or process responsible for initiating the system event. 12 The audit trail shall capture system startup and shutdown functions. 13 The audit trail shall capture modifications to administrator account(s) and administrator group account(s) including: i) escalation of user account privileges commensurate with administrator-equivalent account(s); and ii) adding or deleting users from the administrator group account(s). 14 The audit trail shall capture the enabling or disabling of audit report generation services. 15 The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., OS, application, database). 16 The audit trail shall be protected from unauthorized access, use, deletion or modification. 17 The audit trail shall be restricted to personnel routinely responsible for performing security audit functions.			
50	AU-8	Audit trails are protected from modification, unauthorized access, and destruction.	C:\Windows\SYSTEM32\CONFIG directory → display its contents → view security permissions.	Security permissions for C:\Windows\SYSTEM32\CONFIG -Administrators, Auditors			

51	AU-8	Event logs are configured to be protected from guests.	Using the Microsoft Management Console tool, perform a basic Security Configuration and Analysis. Under the “Security Configuration” section, click “Event Log”, and select “Settings for Event Log”. Inspect the settings for reasonableness.	The event logs should be retained for a significant period of time and cleared manually. Retention should be controlled manually. The event logs should be completely restricted from guest accounts. The computer should shut down in the event of the logs becoming full. • Event logs are restricted from guest access: - HKLM\ System\ CurrentControlSet\ Services\ EventLog\ Application\ RestrictGuestAccess: REG_DWORD : 1 - HKLM\ System\ CurrentControlSet\ Services\ EventLog\ Security\ RestrictGuestAccess: REG_DWORD : 1 - HKLM\ System\ CurrentControlSet\ Services\ EventLog\ System\ RestrictGuestAccess: REG_DWORD : 1			
52	AU-4	Event logs are configured to be retained and protected in the event of becoming full.	Local security settings → Local Security Policies → Security Options → Verify Windows system “Shut Down system immediately if unable to log security alerts”	• "Shut Down system immediately if unable to log security alerts” : - Enabled			
53	IA-3	Password history is maintained for a minimum of six (6) generations.	Using the Local Security Policy tool, review the “Password Policy” section of the Account Policies and determine the computer setting for “Enforce password history”.	• Verify Password Policy “Enforce password history” is: - Six (6) passwords remembered			
54	IA-3	User accounts that are inactive for a period of 90 days are revoked. This includes new user accounts that have never been accessed.	Consult with the system administrator to verify procedures for identifying inactive accounts and blocking/deleting them.	The system administrator reviews the list of user accounts consistently to identify inactive accounts. The system administrator also reviews the list of new user accounts to identify ones that have never been activated.			
55	, IA-1, IA-2, IA-4	User account does not require a password.	1. Open Local Security Policy 2. Check to see if user accounts require a password.	User accounts require a the use of a password.			
56	IA-1, IA-2, IA-4,	Minimum Password Length	1. Open Local Security Policy 2. Ensure Password Length is set to 9 characters.	Password length must be between 8 and 128 characters.			

57	SC-2	The virtual memory pagefile is wiped clean when Windows shuts down.	Using the Local Security Policy tool, review the “Security Options” section of the Local Policies and determine the computer setting for “Clear virtual memory pagefile when system shuts down”.	• Windows 2003 Security Option “Shutdown: Clear Virtual Memory Pagefile” should be: Enabled			
58	SC-2	FTI files and folders, when deleted, are removed from the Recycle Bin immediately.	Select the Programs | Windows NT Explorer. Select Recycle Bin folder by clicking its icon. Click on File | Properties menu item within the Recycle Bin window.	The “Do not move files to the recycle bin. Remove files immediately on delete” is enabled.			
59	AC-4	Information flow enforcement Information	Computer Configuration -> Administrative Templates-> Windows Components -> Intern	Security ZonesL Use only machine settings will be set to enable HKEY-LOCAL-MACHINE Subkey: \Software\Policies\Microsoft\Windows\CurrentVersion\InternetSettings\ Value Name: Secuirty_HKLM-only Type: REG_DWORD Value: 1 The registry value does exist and equals one			
60	AC-12	Does system terminate terminal and remote sessions after a specific period of activity.	Computer Configuration-> Administrative Templates-> Windows Components -> Terminal Services-> Sessions	"Set time limit for active but idle Terminal Services sessions" set to ENABLED "Idle session limit" set to 15 minutes or less			
61	AC-14	Permitted Actions without Identification or Authorization Only actions necessary to accomplish a specific organizational objective may be conducted without Identification and Authorization	Check that windows is configured to prevent anonymous access to unauthorized network share	Network access: Shares that can be accessed anonymously must be empty			

62	AU-5	Response to Audit Processing Failures	Audit: Shut down system immediately if unable to log security audits This policy setting determines whether the computer shuts down immediately if it is unable to log security events. The amount of administrative overhead that was required to enable the Audit: Shut down system immediately if unable to log security audits setting in the LC and EC environments was determined to be too great. Therefore, this policy setting is configured to Disabled in the baseline policy for those environments. However, this policy setting is configured to Enabled in the baseline policy for the SSLF environment because the additional administrative overhead was deemed acceptable to prevent the deletion of events from the Security log unless an administrator specifically chooses to do so.	Setting Legacy Client Enterprise Client Specialized Security – Limited Functionality Audit the access of global system objects Disabled Disabled Disabled Audit the use of Backup and Restore privilege Disabled Disabled Disabled Shut down system immediately if unable to log security audits Disabled Disabled Enabled			
63	AC-5, AC-6	User Rights Configuation	1. Open the local security policy. 2. Move to the User Rights Assignment. 3. Ensure the following User Rights Assignments are assigned. 4. Refer to win2000_appendix.				
64	CM-7, SA-9	Unnecessary services are run on the system.	1. Look at the services running on the local machine and compare them to win2000_appendix. 2. Ensure that the appropriate services are disabled.				
65	CM-4	The system is formatted with the Windows NT file system (NTFS) for all partitions.	Using the Disk Manager tool, view the logical volumes.	The Disk Manager should show NTFS for all local file systems.			
66	CM-4	IP forwarding and IP source routing have been disabled.	Logon to the Windows machine as an administrative user and execute the Registry Editor. Locate the “HKEY_LOCAL_MACHINE | System | CurrentControlSet | Services | Tcpip | Parameters” folder and locate the “IPEnableRouter” key.	• Locate “HKEY_LOCAL_MACHINE | System | CurrentControlSet | Services | Tcpip | Parameters” verify key setting: - Windows 2003 registry key “IPEnableRouter” should have a value of “0” - Windows 2003 registry key “DisableSourceRouting” should have a value of “1”			

67	CM-4	The system is free of irrelevant files and registry entries.	Using Windows Explorer, display the contents of the following directories: • C:\WINNT\system32\dllcache; C:\WINNT\system32\os2; C:\WINNT\system32 Additionally, execute the Registry Editor and locate the following keys: • HKLM\System\CurrentControlSet\Control \Session Manager\Environment\Os2LibPath • HKLM\System\CurrentControlSet\Control \Session Manager\Subsystems\Optional • HKLM\System\CurrentControlSet\Control \Session Manager\Subsystems\OS2 and • HKLM\System\CurrentControlSet\Control \Session Manager\Subsystems\ POSIX	• “C:\WINNT\system32\dllcache” should not contain: a. os2.exe, os2ss.exe, os2srv.exe, psxss.exe, posix.exe, and psxdll.dll • “C:\WINNT\system32\os2” should not contain: a. os2.exe, os2ss.exe, os2srv.exe, psxss.exe, posix.exe, and psxdll.dll b. The os2 directory should not contain any files or folders with the exception of a dll folder, which must be kept intact for system performance. • Os2LibPath, Optional, OS2, and POSIX registry keys should not exist.			
68	CM-3	The Windows operating system have multi-boot capability.	Double click on the “My Computer” icon on the Desktop. Double click the system partition and locate the boot.ini file. Double click the boot.ini file to open it with notepad. Additionally, using Windows Explorer, explore the root directory of C:\ and D:\.	• In boot.ini, under “[operating systems], only two lines should be listed: Multi(0)disk(0)rdisk(0)partition(1)\WINNT=”Windows XP Professional” Multi(0)disk(0)rdisk(0)partition(1)\WINNT=”Windows XP Professional [VGA mode]/basevideo/sos” • In the root directory of C:\ and D:\ only one instance of the directories \Windows, \WinNT32, and \WinNT should exist			
69	CM-3	The Task Scheduler and NT Messenger services are correctly configured.	Using the Microsoft Management Console tool, perform a basic Security Configuration and Analysis. Under the “Security Configuration” section, click System Services, and locate Messenger and NT Task Scheduler. Right click on both of these items, select “Security”, select “View Security”, and select “Advanced”.	The following permissions should be set for Administrator and System: Administrators Query Configuration Query Status Enumerate dependents Stop Interrogate Read System Read Start Stop			
70	CM-3	The DirectDraw access to video hardware and memory is disabled.	Logon to the Windows machine as an administrative user and execute the Registry Editor. Navigate to HKLM | SYSTEM | CurrentControlSet | Control | GraphicsDrivers | DCI and observe the value for “Timeout” (REG_DWORD).	• Locate “HKLM | SYSTEM | CurrentControlSet | Control | GraphicsDrivers | DCI” and verify registry value for “Timeout” is set to zero “0”.			
	AC-5, AC-6	User Rights Configuration	1. Open thye local security policy. 2. Move to the User Rights Assignment. 3. Ensure the following User Rights Assignments are assigned. 4. Refer to win20030-appendix.	Ensure the User Rights Assignments follow what is in the test steps. Refer to Appendix B for more information.			

Comments/Supporting

NIST ID (800-53/A)	Test Objective	Test Steps / Expected Results			Pass /Fail	Actual Results	Comments/Supporting Evidence
AC-6	Proper permissions are established for system files and folders.	Procedures: Using the Local Security Policy tool, review the “User Rights Assignment” section of the Local Policies. Expected Results: • The user rights displayed are consistent with those listed below for Windows 2000.					
		File/Folder Name	**User Groups**	**Permissions**			
		%SystemDirectory%\	Administrators	Full Control			
			Creator Owner	Full Control			
			(subfolders and files)	Full Control			
			System	Read & Execute			
			Auth Users				
		%SystemDirectory%\appmgnt	Administrators	Full Control			
			Creator Owner	Full Control			
			System	Full Control			
			Auth Users	Read & Execute			
		%SystemDirectory%\config\	Administrators	Full Control			
			System	Full Control			
		%SystemDirectory%\dllcache	Administrators	Full Control			
			Creator Owner	Full Control			
			System	Full Control			
		%SystemDirectory%\DTCLog	Administrators	Full Control			
			Creator Owner	Full Control			
			System	Full Control			
			Users	Read, Execute			
		%SystemDirectory%\GroupPolicy	Administrators	Full Control			
			System	Full Control			
			Auth Users	Read, Execute			
		%SystemDirectory%\ias	Administrators	Full Control			
			Creator Owner	Full Control			
			System	Full Control			
		%SystemDirectory%\Ntbackup.exe	Administrators	Full Control			
			Systems	Full Control			
		%SystemDirectory%\NTMSData	Administrators	Full Control			
			Systems	Full Control			
		%SystemDirectory%\rcp.exe	Administrators	Full Control			
			Systems	Full Control			
		%SystemDirectory%\Regedt32.exe	Administrators	Full Control			
			Systems	Full Control			
		%SystemDirectory%\Reinstall Backups	Ignore	Ignore			
		File/Folder Name	**User Groups**	**Permissions**			

%SystemDirectory%\repl (DC only)	Administrators	Full Control				
	Systems	Full Control				
	Users	Read, Execute				
%SystemDirectory%\repl\import	Administrators	Full Control				
	Systems	Full Control				
	Replicator	Modify				
	Users	Read, Execute				
%SystemDirectory%\repl\export	Administrators	Full Control				
	Systems	Full Control				
	Replicator	Read, Execute				
	Users	Read, Execute				
%SystemDirectory%\rexec.exe	Administrators	Full Control				
	Systems	Full Control				
%SystemDirectory%\rsh.exe	Administrators	Full Control				
	System	Full Control				
%SystemDirectory%\secedit.exe	Administrators	Full Control				
	Systems	Full Control				
%SystemDirectory%\Setup	Administrators	Full Control				
	Systems	Full Control				
	Users	Read, Execute				
%SystemDirectory%\spool\Printers	Administrators	Full Control				
	Creator Owner	Full Control				
	(subfolders and files)					
	System	Full Control				
	Users	Traverse folder, Read extended attributes,				
	(folders & subfolders)					
%SystemDrive%	Administrators	Full Control				
	Creator Owner	Full Control				
	(subfolders and files)					
	System	Full Control				
	Auth Users	Modify				
	(Workstations Only)					
%SystemDrive%\ ntdetect.com	Administrators	Full Control				
	Systems	Full Control				
%SystemDrive%\ ntldr.sys	Administrators	Full Control				
	System	Full Control				
%SystemDrive%\ntbootdd.sys	Administrators	Full Control				
	Systems	Full Control				
%SystemDrive%\autoexec.bat	Administrators	Full Control				
	System	Full Control				
	Users	Read, Execute				
File/Folder Name	**User Groups**	**Permissions**				
%SystemDrive%\boot.ini	Administrators	Full Control				
	System	Full Control				
%SystemDrive%\config.sys	Administrators	Full Control				
	System	Full Control				

	Users	Read, Execute			
%SystemDrive%\Documents and Settings	Administrative	Full Control			
	System	Full Control			
	Users	Read, Execute			
%SystemDrive%\ Documents and Settings\Administrator	Administrators	Full Control			
	System	Full Control			
%SystemDrive%\ Documents and Settings\All Users	Administrators	Full Control			
	System	Full Control			
	Users	Read, Execute			
%SystemDrive%\ Documents and Settings\Default User	Administrators	Full Control			
	System	Full Control			
	Users	Read, Execute			
%SystemDrive%\ Documents and Settings\All Users\Documents\DrWatson	Administrators	Full Control			
	Creator Owner	Full Control			
	(subfolders and files)				
	System	Full Control			
	Users	Traverse Folders, Create Files, Create Folders			
	(subfolders and files)	Read, Execute			
	Users				
%SystemDrive%\ Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log	Administrators	Full Control			
	Creator Owner	Full Control			
	System	Full Control			
	Users	Modify			
%SystemDrive%\Inetpub	Ignore	Ignore			
%SystemDrive%\io.sys	Administrators	Full Control			
	System	Full Control			
	Users	Read, Execute			
%SystemDrive%\Msdos.sys	Administrators	Full Control			
	System	Full Control			
	Users	Read, Execute			
File/Folder Name	**User Groups**	**Permissions**			
%SystemDrive%\My Download Files	Administrators	Full Control			
	Creator Owner	Full Control			
	(subfolders and files)				
	System	Full Control			
	Users	Read, Execute			
%SystemDrive%\Program Files	Administrators	Full Control			
	System	Full Control			
	Creator Owner	Full Control			
	(subfolders and files)				
	Auth Users	Modify			

%SystemDrive%\System volume information	Ignore	Ignore				
%SystemDrive%\Temp	Administrators	Full Control				
	Create Owner	Full Control				
	(subfolders and files)					
	System	Full Control				
	Users	Traverse folder, Create files, Create folders				
	(folders and subfolders)					
%SystemRoot%	Administrators	Full Control				
	Creator Owner	Full Control				
	(subfolders and files)					
	System	Full Control				
	Auth Users	Read, Write, Execute				
	(folder only)					
	Auth Users	Read, Execute				
	(subfolders and files)					
%SystemRoot%/Repair	Administrators	Full Control				
	System	Full Control				
%SystemRoot%/Security	Administrators	Full Control				
	Creator Owner	Full Control				
	(subfolders and files)					
	System	Full Control				
%SystemRoot%\$NTServicePackUninstall$	Administrators	Full Control				
	System	Full Control				
%SystemRoot%\$NTUninstall* (all uninstall folders)	Administrators	Full Control				
	System	Full Control				
File/Folder Name	**User Groups**	**Permissions**				
%SystemRoot%\debug	Administrators	Full Control				
	Creator Owner	Full Control				
	(subfolders and files)					
	Systems	Full Control				
	Users	Read, Execute				
%SystemRoot%\debug\UserMode	Administrators	Full Control				
	System	Full Control				
	Users	Traverse Folder, List Folder, Create Files				
	(folder only)					
		Create files, Create folders				
	Users					
	(files only)					
%SystemRoot%\Help	Administrators	Full Control				
	Creator Owner	Full Control				
	System	Full Control				

			Auth Users	Read, Write, Execute			
		%SystemRoot%\NTDS	Administrators	Full Control			
			System	Full Control			
		%SystemRoot%\Offline Web Pages	Ignore	Ignore			
		%SystemRoot%\Regedit.exe	Administrators	Full Control			
			System	Full Control			
			Auth Users	Read, Execute			
			(Workstations only)				
		%SystemRoot%\Registration	Administrators	Full Control			
			Systems	Full Control			
			Users	Read			
		%SystemRoot%\SYSVOL	Administrators	Full Control			
			System	Full Control			
			Creator Owner	Full Control			
			(sub-folders and files)				
			Auth Users	Read, Execute			
		%SystemRoot%\SYSVOL\Domain Policies	Administrators	Full Control			
			System	Full Control			
			Authenticated Users	Read, Execute			
			Creator Owner	Full Control			
			(subfolders and files)				
			Group Policy Creator Owner	Modify			
		File/Folder Name	**User Groups**	**Permissions**			
		%SystemRoot%\Tasks	Ignore	Ignore			
		%SystemRoot%\Temp	Administrators	Full Control			
			Creator Owner	Full Control			
			(subfolders and files)				
			System	Full Control			
			Users	Traverse folder, Create files, Create folders			
			(folders and subfolders)				
AC-2	Permissions for registry keys are set properly.	Procedures: Using the Local Security Policy tool, review the “User Rights Assignment” section of the					
		Registry Key	**User Groups**	**Permissions**			
		Classes_Root	Administrators	Full Control			
			Creator Owner	Full Control			
			(subkeys only)				
			System	Full Control			
			Auth Users	Read			
		Classes_Root\.hlp	Administrators	Full Control			
			System	Full Control			
			Creator Owner	Full Control			
			(subkeys only)				
			Auth Users	Read			
		Classes_Root\helpfile	Administrators	Full Control			

	System	Full Control			
	Auth Users	Read			
HKLM\Software	Administrators	Full Control			
	Creator Owner	Full Control			
	(subkeys only)				
	System	Full Control			
	Auth Users	Read			
HKLM\Software\ Windows 3.1 Migration Status	Administrators	Full Control			
(key only)	Creator Owner	Full Control			
	System	Full Control			
	Auth Users	Read			
HKLM\Software\Microsoft\ Windows	Administrators	Full Control			
	System	Full Control			
	Auth Users	Read, Write			
HKLM\Software\Microsoft\ Windows \CurrentVersion\Group Policy	Administrators	Full Control			
	System	Full Control			
	Auth Users	Read			
Registry Key	**User Groups**	**Permissions**			
HKLM\Software\Microsoft\ Windows \CurrentVersion\Installer	Administrators	Full Control			
	System	Full Control			
	Auth Users	Read			
HKLM\Software\Microsoft\ Windows \CurrentVersion\Policies	Administrators	Full Control			
	System	Full Control			
	Auth Users	Read			
HKLM\Software\Microsoft\ Windows \CurrentVersion\Run	Administrators	Full Control			
	Creator Owner	Full Control			
	System	Full Control			
	Auth User	Read			
HKLM\Software\Microsoft\ Windows NT	Administrators	Full Control			
(key only)	Creator Owner	Full Control			
	System	Full Control			
	Auth User	Read			
HKLM\Software\Microsoft\ Windows NT \CrrentVersion\AEDebug	Administrators	Full Control			
(key only)	System	Full Control			
	Auth User	Read			
HKLM\Software\Microsoft\ Windows NT \CurrentVersion\AsrCommands	Administrators	Full Control			
	Backup Operator	Query, Set Value, Create Subkey, Enumerate, Notify, Delete, Read			
		Full Control			
		Full Control			
	Creator Owner	Read			
	(subkeys only)				
	System				
	Users				

HKLM\Software\Microsoft\ Windows NT \CurrentVersion\Compatability	Administrators	Full Control			
(key only)	Creator Owner	Full Control			
	System	Full Control			
	Auth User	Read			
Registry Key	**User Groups**	**Permissions**			
HKLM\Software\Microsoft\ Windows NT \CurrentVersion\Font Drivers	Administrators	Full Control			
(key only)	Creator Owner	Full Control			
	System	Full Control			
	Auth User	Read			
HKLM\Software\Microsoft\ Windows NT \CurrentVersion\FontMapper	Administrators	Full Control			
(key only)	Creator Owner	Full Control			
	System	Full Control			
	Auth User	Read			
HKLM\Software\Microsoft\ Windows NT \CurrentVersion\Image File Execution Options	Administrators	Full Control			
(key only)	Creator Owner	Full Control			
	System	Full Control			
	Auth User	Read			
HKLM\Software\Microsoft\ Windows NT \CurrentVersion\IniFileMapping	Administrators	Full Control			
(key only)	Creator Owner	Full Control			
	System	Full Control			
	Auth User	Read			
HKLM\Software\Microsoft\ Windows NT \CurrentVersion\PerfLib	Administrators	Full Control			
	Creator Owner	Full Control			
	System	Full Control			
	Interactive	Read			
HKLM\Software\Microsoft\ Windows \CurrentVersion\RunOnce	Administrators	Full Control			
	Creator Owner	Full Control			
	System	Full Control			
	Auth User	Read			
HKLM\Software\Microsoft\ Windows \CurrentVersion\RunOnceEx	Administrators	Full Control			
	Creator Owner	Full Control			
	System	Full Control			
	Auth User	Read			
Registry Key	**User Groups**	**Permissions**			
HKLM\Software\Microsoft\Windows\Current Version\Uninstall	Administrators	Full Control			
	Creator Owner	Full Control			
	System	Full Control			
	Auth User	Read			
HKLM\Software\Microsoft\ Windows NT \CurrentVersion\Winlogon	Administrators	Full Control			
	Creator Owner	Full Control			
	System	Full Control			
	Auth User	Read			
HKLM\Software\Microsoft\Cryptography	Administrators	Full Control			
(key only)	System	Full Control			
	Auth User	Read			
HKLM\Software\Microsoft\NetDDE	Administrators	Full Control			
	System	Full Control			

HKLM\Software\Microsoft\OLE	Administrators	Full Control			
	System	Full Control			
	Auth User	Read			
HKLM\Software\Microsoft\OS/2 Subsystem for NT	Administrators	Full Control			
	Creator Owner	Full Control			
	System	Full Control			
HKLM\Software\Microsoft\Protected Storage System Provider	Ignore	Ignore			
HKLM\Software\Microsoft\RPC	Administrators	Full Control			
	System	Full Control			
	Auth User	Read			
HKLM\Software\Program Groups	Administrators	Full Control			
	Creator Owner	Full Control			
	System	Full Control			
	Auth User	Read			
HKLM\Software\Secure	Administrators	Full Control			
(key only)	Creator Owner	Full Control			
	System	Full Control			
	Auth User	Read			
HKLM\System	Administrators	Full Control			
	Creator Owner	Full Control			
	(subkeys only)				
	System	Full Control			
	Auth Users	Read			
HKLM\System\clone	Ignore	Ignore			
Registry Key	**User Groups**	**Permissions**			
HKLM\System\controlset001 – through – HKLM\System\controlset010	Administrators	Full Control			
	Creator Owner	Full Control			
	(subkeys only)				
	System	Full Control			
	Auth User	Read			
HKLM\System\CurrentControlSet\ Services\UPS	Administrators	Full Control			
(key only)	Creator Owner	Full Control			
	System	Full Control			
	Auth User	Read			
HKLM\System\CurrentControlSet\ Control\WMI\Security	Administrators	Read			
	Creator Owner	Full Control			
	System	Full Control			
HKLM\System\CurrentControlSet\Control\SecurePipeServers\winreg	Administrators	Full Control			
	System	Full Control			
Note: *MS Exchange Server requires remote Registry access. Therefore, on Exchange Servers and domain controllers within the domain, add the Domain Exchange Servers group with Full Control access on this Registry key.*	Backup Operator	Read			
	(keys only)				
HKLM\System\CurrentControlSet\Enum	Ignore	Ignore			
HKLM\System\CurrentControlSet\Hardware	Administrators	Full Control			

		Profiles	Creator Owner	Full Control			
			(subkeys only)				
			System	Full Control			
			Auth Users	Read			
		Registry Key	**User Groups**	**Permissions**			
		HKLM\System\CurrentControlSet\Services\ LanManServer\	Administrators	Full Control			
			System	Full Control			
		Note: *For workstations, look for LanManWorkstation instead of LanManServer.*	Auth User	Read			
		HKLM\System\CurrentControlSet\Services\ SNMP\Parameters\PermittedManagers	Administrators	Full Control			
			Creator Owner	Full Control			
			System	Full Control			
		HKLM\System\CurrentControlSet\Services\ SNMP\Parameters\Valid Communities	Administrators	Full Control			
			Creator Owner	Full Control			
			System	Full Control			
		Users\.Default\	Administrators	Full Control			
			Creator Owner	Full Control			
			(subkeys only)				
			System	Full Control			
			Auth User	Read			
		Users\.Default\Software\Microsoft\NetDDE	Administrators	Full Control			
			System	Full Control			
		sers\.Default\Software\Microsoft\Protected Storage Systems Provider	Ignore	Ignore			
		Users\.Default\Software\Microsoft\Windows \CurrentVersion\Policies	Administrators	Full Control			
			Creator Owner	Full Control			
			System	Full Control			
			Auth Users	Read			
AC-6	Only authorized users are able to perform administrative tasks that can affect system security. General user accounts do not have administrator privileges.	Procedures: Using the Local Security Policy tool, review the “User Rights Assignment” section of the Local Policies. Expected Results:					
		Policy	**Expected Settings**				
		Access this computer from the network	Administrators				
		Act as part of the operating system	No One				
		Add workstations to the domain	Not Defined				
		Adjust memory quotas for a process (2003)	Not Defined				
		Allow log on locally (2003)	Administrators				
		Allow log on through terminal services (2003)	Administrators				
		Backup files and directories	Administrators, Backup Operators				
		Bypass traverse checking	Authenticated Users				
		Change the system time	Administrators				
		Create a page-file	Administrators				
		Create a token object	No One				
		Create global objects (2003)	Not defined				

Create permanent shared object	No One					
Debug programs	No One					
Deny access to this computer from the network	Anonymous logon, Guest					
Deny logon as a batch job	No One					
Deny logon as a service	No One					
Deny logon locally	No One					
Deny logon through terminal service (2003)	Not defined					
Policy	**Expected Settings**					
Enable computer and user accounts to be trusted for delegation	No One					
Force shutdown from a remote system	Administrators					
Generate Security Audits	Local Service, Network Service					
Impersonate a client after authentication (2003)	Service					
Increase quotas	Administrators					
Increase scheduling priority	Administrators					
Load and unload device drivers	Administrators					
Lock pages in memory	No One					
Log on as a batch job	No One					
Log on as a service	As needed					
Log on locally	Administrator, (other specific users)					
Manage auditing and security log	Administrators					
Modify firmware environment values	Administrators					
Perform volume maintenance tasks (2003)	Administrators					
Profile single process	Administrators					
Profile system performance	Administrators					
Remove computer from docking station	Administrators and Authenticated Users (for workstations)					
Replace a process level token	Network Service, Local Service					
Restore files and directories	Administrators, Backup Operators					
Shut down the system	Administrators					
Synchronize directory service data	No One					
Take ownership of files or other objects	Administrators					

Test ID	NIST ID (800-53/A)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments/ Supporting Evidence
1	AU-2, AU-3,	Auditing is configured to capture information including: date, time, files, user, success/ failure, and type about security relevant events.	Within the User Manager for Domain window, select Policies | Audit menu option. Verify that Audit policy is configured as prescribed below. Policy: Expected Setting Logon and Logoff: Success/Failure Files and Object Access: Success/Failure Use of User Rights: Success/Failure User and Group Management: Success/Failure Security Policy Changes: Success/Failure Restart, Shutdown and System: Success/Failure Process Checking: None	Within the User Manager for Domain window, select Policies | Audit menu option. Verify that Audit policy is configured as prescribed below.			
2	AU-9	The audit log does not overwrite old events. The system provides a configurable capability to archive audit data.	1. Launch Event Viewer by selecting Programs | Administrative Tools | Event Viewer from the Start menu. Select Log | Log Settings from the menu. In the Event Log Settings windows, verify that "Do Not Overwrite Events" is selected. 2. Verify the "Maximum Log Size" entry. 3. Select "Log" from the menu and select the "Save As .." choice from the "Log" menu item. 4. Launch Explorer and select C:\WINT\SYSTEM32\CONFIG directory. 5. Verify that Audit logs are regularly archived and Check audit configuration status on critical directories.	1. The "event log wrapping" choice "do not overwrite events (clear log manually)" is selected. 2. The "maximum log size" entry is set to 4194240k for servers. 3. The save as dialog box appears allowing the saving of the log to an administrator selected location. 4. Local audit logs are stored in this directory. 5. Security events related to critical directories are captured.			
3	IA-3	Users are forced to change passwords at a maximum of 90 days	Logon as sysadmin and Access Programs Administrative Tools | User Manager (or User Manager for Domains) menu. Select Policies | Account Policy from the User Manager Window. View the settings in the Accounts Policy screen.	Password uniqueness by remembering 6 passwords			
4	, IA-1, IA-2, IA-4	The “Password never expire” checkbox is not checked.	Logon as sysadmin. Click Start button and select Program | Administrative Tools | User Manager (or User Manager for Domain) from menu. Identify all standard accounts in the user list. Right click on these accounts one at a time and select Properties from the menu to open the User Properties window.	Password never expire box is not checked.			
5	AC-2,	User accounts are created at the domain level and all user accounts are in one of the master domains.	Logon as sysadmin at a domain controller. Click on Start button and select Program | Administrative Tools | User Manager for Domain from the menu. Connect to the master domain and browse the user account listings.	Verify that Master Domain contains user accounts.			
6	AC-3	User accounts are not created in resource domains.	Logon as sysadmin at a domain controller. Click on Start button and select Program | Administrative Tools | User Manager for Domain from the menu. Connect to a resource domain and browse user account listings.	Verify that the resource domain does not contain any user accounts except for few Admin accounts.			

7	AC-3	Privileged users within local and global groups are properly grouped to ensure Account Policy is not bypassed.	Review the User Manager for Domains to view the various users and group levels. Review groups looking for segregation of duties (i.e. Power Users, Administrators, and Backup Operators). Make sure privileged users reside in the correct group. (i.e. Power User residing in the Admin. Group)	Privileged users reside in the correct group			
8	AC-11	Current user configuration is not set with a password-protected screen saver.	1. Right-click destop 2. Click properties 3. Click screen saver tab 4. Look to see that there is a password-protected screensaver set and that it is enabled to activate sooner that 15 minutes.	Ensure that a password-protected screensaver is set and that is activated sooner than 15 following inactivity.			
9	SC-3	SYSKEY is installed and enabled.	Logon to the Windows machine as an administrative user and execute "SYSKEY" from the "Run" prompt. Inspect the configuration of SYSKEY.	• The "Enable Encryption" radio button should be checked and the "Disable Encryption" radio button should be unchecked and grayed out.			
10	AU-6	Hardware and firmware elements of the system are routinely monitored using system diagnostic capabilities.	Discuss with System Admin any hardware and/or software features (e.g., firmware diagnostics) provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the system	The System integrates diagnostic software (e.g. Windows Diagnostic, WinTask, Everest, Sun Fire, etc...) routinely used to perform and document system integrity checks on the hardware and firmware components of the Windows operating system. MS Systems Update Server is also recommended but not required to ensure network service packs are distributed in the environment			
11	SC-4	FTI is encrypted during transmission over telecommunication lines.	Evaluate conceptual design of the network architecture. Identify all access points to the system (e.g., mainframe host, server) that store and process FTI. Determine if the use of guided media and or encryption techniques are used to secure FTI transmission over telecommunication lines between "remote" locations and the data center locations housing FTI on the system (mainframe host or server).	Guided media and/or encryption is used during FTI transmission over telecommunication lines. Guided Media: End-to-end unencrypted cable circuits of copper or fiber optics. Encryption: (a) SSL (b) VPN using IPSEC (c) Router-based DES encryption (d) TLS or (e) other viable encryption strategies as deemed appropriate.			
12	AC-4	System users have minimum privileges required to perform their assigned functions, and these privileges are controlled using group structures.	Using the User Administration tool, determine the system's group structure.	The system should be using group structures to aggregate and delegate privileges. A limited number of users should be members of the Administrators, Power Users, and Backup Operators groups. No users should be members of the Guest group, with the exception of the "Guest" account.			

13	AC	Permissions for registry keys are set properly.	1. Launch the Registry editor by typing Regedt32 at the Run prompt. 2. Locate each Registry key listed in the table below and verify its permissions are set as recommended. To list permissions on a Registry key, highlight the key by clicking on it and then click Security | Permissions in the Registry editor menu.	Windows NT Registry are consistent with the "NT Registry" tab.			
14	, SC-4	Terminal Services Temp Folder Deletion	The following registry key does exist and its value is set to 1: Registry Hive: HKEY_LOCAL_MACHINE Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services Value Name: DeleteTempDirsOnExit	The temp folder is deleted when the session terminates.			
15	AC-3	Shared permissions are assigned properly.	1. Launch windows explorer and click right mouse button on a shared folder (hand picture underneath the regular folder icon). Select Properties from the menu. Click on the Sharing tab and click Permissions to verify the permission settings. 2. Settings | Printers from the menu. Identify shared printers (hand picture underneath the regular printer icon). Select shared printer Properties. Click the Security tab, then Permissions button. Verify that permissions are correctly set. 3. Repeat step 2 for all shared printers.	1.Everyone group is not given full control permission on any shares. Authenticated users group is used in place of the everyone group. Users and/or groups are given the minimum amount of permissions needed on a share. 2.Recommended printer share security settings: Authenticated Users: Print Administrators: Full Control System: Full Control Creator Owner: Full Control			
16	AC-3	Proper permissions are set for files and folders (including folders with FTI). System operators have the minimum privileges required to perform their assigned functions. Manual permissions for files and folders are properly set.	1. In the Taskbar, click Start button and select Programs | Windows Explorer from menu. To verify permissions of a file or folder, right click on it, and choose Properties from the pop out menu. In the Properties window, select the Security tab and then click Permissions button. 2. Ensure the following permissions have been set on files and folders within the %SYSTEMDRIVE%: Note: The phrase “folder, subfolder and files” in File System column of the tables below indicate that the permission on the parent folder should be replaced on all subfolders and files in that folder. The phrase “ignore” in the User Group column of following table indicates that the file or folder should retain its default permissions instead of inheriting them from a parent folder.	Windows NT Permissions are consistent with the "NT Permissions" tab.			

17	AC-17	All dial-up access to the Windows NT server is protected with approved devices or techniques that provide explicit identification and authentication and audit trails. Access control in the form of properly administered user name and authentication is established for each user having dial-in access. Dial-in access is allowed only if users are authenticated with hardware tokens and if communications are encrypted.	1. Consult with the system administrator and verify that dial-up access is controlled through security measures. 2. Consult with the system administrator and verify that dial-up access is controlled through identification and authentication and audit trails.	1. Dial-up communications are encrypted. 2. Dial-up access requires user IDs and passwords or hardware tokens. Dial-in access is recorded in audit logs.			
18	AC-17	The telnet session file does not appear in explorer.	Right click on the Start button and select Program | Windows Explorer to launch the Explorer. Navigate to the %SYSYTEMROOT% directory. Verify that the TELNET.EXE file does not exist.	The telnet.exe file does not show in explorer.			
19	, AU-2, AU-3	Registry Auditing	1. From the command line, type REGEDT32. 2. Expand Hkey_Local_Machine. 3. For both the System and Software Registry Keys, Right click System or Software and select Permissions. 4. Click the advanced button then select the Auditing tab. 5. Ensure the Everyone group is set to Full Control for auditing.	Audting is enabled on the HKLM\Software and HKLM\System registry keys.			
20	, AC-8	Legal Notice Logon Banner	1. Open the local security policy. 2. Move to Security Options. 3. The value for "Interactive Logon: Message text for users attempting to log on" includes information on Government Systems and consent to monitoring.	Legal notice contains warnings of consent to monitoring and identifies the system as a government system.			
21	, AU-9	Capturing Audit Events	1. Open the local security policy. 2. Move to Security Options. 3. The site has procedures in place and the value for “Audit: Shut down system immediately if unable to log security audits” is set to “Enabled”.	The value for “Audit: Shut down system immediately if unable to log security audits” is set to “Enabled”			

22	AU-2, AU-3,	Changes to selected Registry keys is audited.	1. Login to the NT server as sysadmin. 2. Launch the Registry editor by typing Regedt32 at the Run prompt. 3. Click on HKEY_LOCAL_MACHINE window to bring it in the foreground and select HKEY_LOCAL_MACHINE | Software | Program Groups window. 4. Click on Security | Auditing menu item. Verify that significant changes to security related Registry keys are audited.	SIGNIFICANT CHANGES ARE AUDITED. (MOST SUBKEYS BELOW WINLOGON AND LSA)			
23	SC-3	FTI files and folders, when deleted, are removed from the Recycle Bin immediately.	Select the Programs | Windows NT Explorer. Select Recycle Bin folder by clicking its icon. Click on File | Properties menu item within the Recycle Bin window.	The “Do not move files to the recycle bin. Remove files immediately on delete” is enabled.			
24	AC-3	The “Everyone” group is removed, and has a new group “Authenticated Users” is created.	Logon as sysadmin. Click Start button and select Program | Administrative Tools | User Manger (or User Manager for Domain) from menu. Identify all standard accounts in the user list.	The authenticated users group is listed in the user manager and everyone group does not exist.			
25	AC-6	The Power Users group does not exist on servers acting as either a PDC or BDC.	Logon as sysadmin. Click Start button and select Program | Administrative Tools | User Manager (or User Manager for Domain) from menu. Identify all standard accounts in the user list.	Verify that the power users group is not listed in the user manager (for domain controllers only).			
26	AC-4	Trust Relationships are limited to one-way trusts unless approved and documented.	Logon at a domain controller as sysadmin. Launch User Manager for Domains program by selecting Programs | Administrative Tools | User Manager for Domains from the Start menu. Within User Manager for Domains window, click Policies | Trust Relationship menu items.	Trust relationships are limited to one-way trust. If not, the same domain name appears in both trusted domain and trusting domain windows. All two-way trust relationships are approved and documented.			
27	AC-4	The PDC has Remote Access Service (RAS) configured and running.	Click on the Start button and select Settings | Control Panel from the menu. Double click on the Network icon in the Control Panel Window to launch network properties window. Click on the Services tab and highlight the Remote Access Server and click on Properties button. When the RAS Properties windows appears, click on Network button and verify that RAS is enablaed secure	RAS configuration is secured.			
28	, SC-9, AC-18	Outgoing Secure Channel Traffic Encryption	1. Open the local security policy. 2. Move to Security Options. 3. The value for “Domain Member: Digitally encrypt secure channel data (when possible)” is set to “Enabled”. 4. The value for “Domain Member: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”.	The value for “Domain Member: Digitally encrypt secure channel data (when possible)” is set to “Enabled”. -or- “Domain Member: Digitally encrypt or sign secure channel data (always)” is set to “Enabled”.			
29	AC-7, AC-9, AC-10	Failed Login Minimum Requirement	1. Open the local security policy. 2. Move to the Account Lockout Policy. 3.The “Account lockout threshold” is NOT “0” or more than three attempts.	The value for If the “Account lockout threshold” is “1” or less than or equal to three attempts.			
30	AC-2,	The built-in guest account is not disabled.	1. Open the local security policy. 2. Move to Security Options. 3. IThe value for “Accounts: Guest account status” is set to ” Disabled."	The value for “Accounts: Guest account status” is set to ” Disabled”.			

31	AU-4	Event logs are configured to be retained and protected in the event of becoming full.	Local security settings → Local Security Policies → Security Options → Verify Windows system “Shut Down system immediately if unable to log security alerts”	• "Shut Down system immediately if unable to log security alerts” : - Enabled			
32	IA-3	Password history is maintained for a minimum of six (6) generations.	Using the Local Security Policy tool, review the “Password Policy” section of the Account Policies and determine the computer setting for “Enforce password history”.	• Verify Password Policy “Enforce password history” is: - Six (6) passwords remembered			
33	IA-3	User accounts that are inactive for a period of 90 days are revoked. This includes new user accounts that have never been accessed.	Consult with the system administrator to verify procedures for identifying inactive accounts and blocking/deleting them.	The system administrator reviews the list of user accounts consistently to identify inactive accounts. The system administrator also reviews the list of new user accounts to identify ones that have never been activated.			
34	CM-4	Subsystem files and directories are removed. Remote-access program executables is removed.	1. Launch Windows Explorer and navigate to %SYSTEMDIRECTORY%.Verify that the POSIX directory does not exist. Also, verify that the “posix.exe” and the “psxss.exe” files do not exist. 2. Verify that the “DHCP” directory does not exist in %SYSTEMDIRECTORY% folder. 3. Verify that the following executables do not exist in %SYSTEMDIRECTORY% folder.	1. Neither the POSIX directory nor the “posix.exe” or the :psxss.exe” files exist. 2. The DHCP directory does not exist. 3. Rcp.exe Rsh.exe Rexec.exe			
35	CM-4	DNS Server Service is disabled.	If a server is not used as a DNS server, it should not be running DNS service. Click on the Start button and select Settings | Control Panel from the menu. Double click on the Network icon in the Control Panel Window to launch network properties window. Click on the Services tab and verify that Microsoft DNS server entry is not listed here.	An entry for Microsoft DNS server is not listed on the services tab.			
36	CM-4	The NT Server Microsoft Peer Web Services does not exist	Click on the Start button and select Settings | Control Panel from the menu. Double click on the Network icon in the Control Panel Window to launch network properties window. Click on the Services tab and verify that MICROSOFT PEER WEB SERVICES is not listed here.	Microsoft peer web services is not present.			
37	CM-4	Unless the machine is used as a web server, Microsoft IIS is not installed on NT server.	Click on the Start button and select Settings | Control Panel from the menu. Double click on the Network icon in the Control Panel Window to launch network properties window. Click on the Services tab and verify that MICROSOFT IIS is not listed here.	IIS IS NOT LISTED.			
38	CM-3	The system is formatted with the Windows NT file system (NTFS) for all partitions.	Using the Disk Manager tool, view the logical volumes.	The Disk Manager should show NTFS for all local file systems.			
39	CM-3	NTFS permissions for server user home directories are set properly.	1. Launch Windows Explorer and click on the drive that contains user’s home directories, or If user’s home directories reside on another machine, connect to that server through C$ administrative share and locate the drive that contains user’s home directories. Right click on few home directories randomly and verify that their permissions are properly set.	Permissions for server user home directories are set as follows: Domain administrators –read Owner (username) – full control System -- full control			

40	CM-4	IP forwarding and IP source routing have been disabled.	Click on Start button and select Settings| Control Panel to open the Control Panel window. Click on the Network icon to launch Network Properties box. Click on the Protocol tab, highlight TCP/IP and click on the Properties button. Click on the Routing tab in the Microsoft TCP Properties window. Verify that IP forwarding box is not checked.	IP forwarding box is not checked on routing tab of Microsoft TCP/IP properties box.			
41	CM-2	Deletions within the registry are confirmed.	Logon as sysadmin. Click the Start button and select Run from the pop-up menu. Type in regedt32.exe at the Run prompt and hit <Enter> key. Click on Options menu item within the Registry editor window and verify that Confirm on Delete menu option is checked.	"CONFIRM ON DELETE" is checked			
42	CM-3	The Windows operating system have multi-boot capability.	Double click on the "My Computer" icon on the Desktop. Double click the system partition and locate the boot.ini file. Double click the boot.ini file to open it with notepad. Additionally, using Windows Explorer, explore the root directory of C:\ and D:\.	• In boot.ini, under "[operating systems], only two lines should be listed: Multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Workstation 4.0" Multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Workstation 4.0 [VGA mode]/basevideo/sos" • In the root directory of C:\ and D:\ only one instance of the directories \Windows, \WinNT32, and \WinNT should exist			
43	AC-5, AC-6	User Rights Configuration	1. Open thye local security policy. 2. Move to the User Rights Assignment. 3. Ensure the following User Rights Assignments are assigned. 4. Refer to win2003-appendix.	Ensure the User Rights Assignments follow what is in the test steps. Refer to Appendix B for more information.			
44	AC-5, AC-6	User Rights Configuration	1. Open thye local security policy. 2. Move to the User Rights Assignment. 3. Ensure the following User Rights Assignments are assigned. 4. Refer to winnt-appendix.	Ensure the User Rights Assignments follow what is in the test steps. Refer to Appendix B for more information.			

NIST ID (800-53/A)	Test Objective	Test Steps / Expected Results			Actual Results	Pass /Fail	Comments/Supporting Evidence
AC-3	Permissions for registry keys are set properly	Procedures: 1. Launch the Registry editor by typing Regedt32 at the Run prompt. 2. Locate each Registry key listed in the table below and verify its permissions are set as recommended. To list permissions on a Registry key, highlight the key by clicking o					
		Registry	**User Groups**	**Permissions**			
		1. CLASSES_ROOT\	Administrators	Full Control			
			Authenticated Users	Read, Write, Execute			
		(keys and sub-keys)	CREATOR OWNER	Full Control			
			SYSTEM	Full Control			
		2. CLASSES_ROOT\.hlp	Administrators	Full Control			
		Key	Authenticated Users	Read, Execute			
			SYSTEM	Full Control			
		3. CLASSES_ROOT\helpfile	Administrators	Full Control			
			Authenticated Users	Read, Execute			
		(keys and sub-keys)	SYSTEM	Full Control			
		4. MACHINE\HARDWARE	Administrators	Full Control			
			Authenticated Users	Read, Write, Execute			
		(keys and sub-keys)	CREATOR OWNER	Full Control			
			SYSTEM	Full Control			
		5. MACHINE\SOFTWARE	Administrators	Full Control			
			Authenticated Users	Read, Write, Execute, Delete			
		(keys and sub-keys)		Full Control			
			CREATOR OWNER	Full Control			
			SYSTEM				
		6. MACHINE\SOFTWARE\Classes	Ignore				
		(keys and sub-keys)					
		7. MACHINE\SOFTWARE\Microsoft\ Cryptography	Administrators	Full Control			
			Authenticated Users	Read, Execute			
		(keys and sub-keys)	SYSTEM	Full Control			
		8. MACHINE\SOFTWARE\Microsoft\ NetDDE	Administrators	Full Control			
			SYSTEM	Full Control			

(keys and sub-keys)			
9. MACHINE\SOFTWARE\Microsoft\ Ole	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	CREATOR OWNER	Full Control	
	SYSTEM	Full Control	
10. MACHINE\SOFTWARE\Microsoft\ OS/2 Subsystem for NT	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	CREATOR OWNER	Full Control	
	SYSTEM	Full Control	
11. MACHINE\SOFTWARE\Microsoft\ Protected Storage System Provider	Ignore		
(keys and sub-keys)			
12. MACHINE\SOFTWARE\Microsoft\ RPC	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	SYSTEM	Full Control	
13. MACHINE\SOFTWARE\Microsoft\ Secure	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	CREATOR OWNER	Full Control	
	SYSTEM	Full Control	
14. MACHINE\SOFTWARE\Microsoft\ Windows	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	CREATOR OWNER	Full Control	
	SYSTEM	Full Control	
15. MACHINE\SOFTWARE\Microsoft\ Windows\	Administrators	Full Control	
Current Version\Run	Authenticated Users	Read, Execute	
	SYSTEM	Full Control	
(keys and sub-keys)			
16	Administrators	Full Control	
MACHINE\SOFTWARE\Microsoft\ Windows\	Authenticated Users	Read, Execute	
Current Version\RunOnce	SYSTEM	Full Control	
(keys and sub-keys)			

17. MACHINE\SOFTWARE\Microsoft\ Windows\	Administrators	Full Control	
Current Version\RunOnceEx	Authenticated Users	Read, Execute	
	SYSTEM	Full Control	
(keys and sub-keys)			
18. MACHINE\SOFTWARE\Microsoft\ Windows\	Administrators	Full Control	
Current Version\Shell Extensions	Authenticated Users	Read, Execute	
	CREATOR OWNER	Full Control	
(keys and sub-keys)	SYSTEM	Full Control	
19. MACHINE\SOFTWARE\Microsoft\ Windows\	Administrators	Full Control	
CurrentVersion\Uninstall	Authenticated Users	Read, Execute	
	CREATOR OWNER	Full Control	
(keys and sub-keys)	SYSTEM	Full Control	
20. MACHINE\SOFTWARE\Microsoft\ Windows NT	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	CREATOR OWNER	Full Control	
	SYSTEM	Full Control	
21. MACHINE\SOFTWARE\Microsoft\ Windows NT\ CurrentVersion\AEDebug	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	SYSTEM	Full Control	
22. MACHINE\SOFTWARE\Microsoft\ Windows NT\ Current Version\Compatibility	Authenticated Users	Read, Write, Execute	
(keys and sub-keys)	CREATOR OWNER	Full Control	
	SYSTEM	Full Control	
23. MACHINE\SOFTWARE\Microsoft\ Windows NT\ CurrentVersion\Font Drivers	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	SYSTEM	Full Control	
24. MACHINE\SOFTWARE\Microsoft\ Windows NT\ CurrentVersion|Font Mapper	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	SYSTEM	Full Control	

25. MACHINE\SOFTWARE\Microsoft\ Windows NT\ CurrentVersion\Image File Execution Options	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	SYSTEM	Full Control	
26. MACHINE\SOFTWARE\Microsoft\ Windows NT\ CurrentVersion\IniFileMapping	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	SYSTEM	Full Control	
27. MACHINE\SOFTWARE\Microsoft\ Windows NT\ CurrentVersion\Perflib	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	SYSTEM	Full Control	
28. MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\Perflib\009	Ignore		
(keys and sub-keys)			
29. MACHINE\SOFTWARE\Microsoft\ Windows NT\ CurrentVersion\Time Zones	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	SYSTEM	Full Control	
30. MACHINE\SOFTWARE\Microsoft\ Windows NT\ CurrentVersion\Winlogon	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	SYSTEM	Full Control	
31. MACHINE\SOFTWARE\Program Groups	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	CREATOR OWNER	Full Control	
	SYSTEM	Full Control	
32. MACHINE\SOFTWARE\Secure	Administrators	Full Control	
	Authenticated Users	Read, Execute	
(keys and sub-keys)	CREATOR OWNER	Full Control	
	SYSTEM	Full Control	
33. MACHINE\SOFTWARE\Windows 3.1 Migration Status	Administrators	Full Control	
	Authenticated Users	Read, Execute	

		(keys and sub-keys)	CREATOR OWNER	Full Control			
			SYSTEM	Full Control			
		34. MACHINE\SYSTEM\CurrentControlSet\Services\Control\SecurePipeServers\winreg	Administrators	Full Control			
			SYSTEM	Full Control			
		(keys and sub-keys)					
		35. MACHINE\SYSTEM\CurrentControlSet\Services\	Administrators	Full Control			
		LanmanServer\Shares	Authenticated Users	Read, Execute			
			CREATOR OWNER	Full Control			
		(keys and sub-keys)	SYSTEM	Full Control			
		36. MACHINE\SYSTEM\CurrentControlSet\Services\	Administrators	Full Control			
		Schedule	Authenticated Users	Read, Execute			
			CREATOR OWNER	Full Control			
		(keys and sub-keys)	SYSTEM	Full Control			
		37. MACHINE\SYSTEM\CurrentControlSet\Services\UPS	Administrators	Full Control			
			Authenticated Users	Read, Execute			
		(keys and sub-keys)	CREATOR OWNER	Full Control			
			SYSTEM	Full Control			
		38. USERS\.DEFAULT	Administrators	Full Control			
			Authenticated Users	Read, Execute			
		(keys and sub-keys)	SYSTEM	Full Control			
		39. USERS\.DEFAULT\Software\Microsoft\NetDDE	Administrators	Full Control			
			SYSTEM	Full Control			
		(keys and sub-keys)					
		40. USERS\.DEFAULT\Software\Microsoft\Protected Storage Systems Provider	Ignore				
		(keys and sub-keys)					
		41. USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies	Administrators	Full Control			
			Authenticated Users	Read, Execute			
		(keys and sub-keys)	CREATOR OWNER	Full Control			
			SYSTEM	Full Control			

AC-6	Proper permissions are set for files and folders. (including folders with FTI) The system operators have the minimum privileges required to perform their assigned functions. Manual permissions for files and folders are properly set.	Procedures: 1. In the Taskbar, click Start button and select Programs | Windows Explorer from menu. To verify permissions of a file or folder, right click on it, and choose Properties from the pop out menu. In the Properties window, select the Security t					
		File System (Folder or File)	**User Groups**	**Permissions**			
		1. %SystemDrive%	Administrators	Full Control			
			Authenticated Users	Read, Write, Execute			
		(folder, subfolders, & files)	CREATOR OWNER	Full Control			
			SYSTEM	Full Control			
		2. %SystemDrive%\autoexec.bat file	Administrators	Full Control			
			Authenticated Users	Read, Execute			
			SYSTEM	Full Control			
		3. %SystemDrive%\boot.ini file	Administrators	Full Control			
			SYSTEM	Full Control			
		4. %SystemDrive%\config.sys file	Administrators	Full Control			
			Authenticated Users	Read, Execute			
			SYSTEM	Full Control			
		5. %SystemDrive%\io.sys file	Administrators	Full Control			
			Authenticated Users	Read, Execute			
			SYSTEM	Full Control			
		6. %SystemDrive%\msdos.sys file	Administrators	Full Control			
			Authenticated Users	Read, Execute			
			SYSTEM	Full Control			
		7. %SystemDrive%\ntdetect.com file	Administrators	Full Control			
			SYSTEM	Full Control			
		8. %SystemDrive%\ntldr file	Administrators	Full Control			
			SYSTEM	Full Control			
		9. %SystemDrive%\NTReskit	Administrators	Full Control			
			Authenticated Users	Read, Execute			
		(folder, subfolders, & file)	CREATOR OWNER	Full Control			
			SYSTEM	Full Control			
		10. %SystemDrive%\pagefile.sys file	Ignore				
		11. %SystemDrive%\Program	Administrators	Full Control			
			Authenticated Users	Read, Write, Execute			
		(folder, subfolders, & files)	CREATOR OWNER	Full Control			
			SYSTEM	Full Control			
		12. %SystemDrive%\Temp	Administrators	Full Control			
			Authenticated Users	Read, Write, Execute			
		(folder, subfolders, & files)	CREATOR OWNER	Full Control			
			SYSTEM	Full Control			
		13. %SystemDrive%\Users\username	User Name	Full Control			
			SYSTEM	Full Control			

(folder, subfolders, & files)					
14. %SystemDrive%\Win32app	Ignore				
(folder, subfolders, & files)					
A. Ensure that access control permissions are set on the following subfolders and					
1. %SystemRoot% folder	Administrators	Full Control			
	Authenticated Users	Read, Write, Execute			
	CREATOR OWNER	Full Control			
	SYSTEM	Full Control			
2. %SystemRoot%	Administrators	Full Control			
	Authenticated Users	Read, Execute			
(subfolders & files)	CREATOR OWNER	Full Control			
	SYSTEM	Full Control			
3. %SystemRoot%\$NtServicePackUninstall$	Administrators	Full Control			
	SYSTEM	Full Control			
(folder, subfolders, & files)					
4. %SystemRoot%\Cookies	Administrators	Full Control			
	Authenticated Users	Read, Write, Execute			
(folder, subfolders, & files)	CREATOR OWNER	Full Control			
	SYSTEM	Full Control			
5. %SystemRoot%\drwtsn32.log file	Administrators	Full Control			
	Authenticated Users	Modify			
	CREATOR OWNER	Full Control			
	SYSTEM	Full Control			
6. %SystemRoot%\Help	Administrators	Full Control			
	Authenticated Users	Read, Write, Execute			
(folder, subfolders, & files)	CREATOR OWNER	Full Control			
	SYSTEM	Full Control			
7. %SystemRoot%\History	Administrators	Full Control			
	Authenticated Users	Read, Write, Execute			
(folder, subfolders, & files)	CREATOR OWNER	Full Control			
	SYSTEM	Full Control			
8. %SystemRoot%\maplud.ini file	Administrators	Full Control			
	Authenticated Users	Modify			
	CREATOR OWNER	Full Control			
	SYSTEM	Full Control			
9. %SystemRoot%\nsreg.dat file	Administrators	Full Control			
	Authenticated Users	Modify			
	CREATOR OWNER	Full Control			
	SYSTEM	Full Control			
10. %SystemRoot%\Profiles	Administrators Authenticated Users	Full Control			
	Creator Owner	Read, Execute			

(folder, subfolders, & files)	SYSTEM	Full Control			
		Full Control			
11. %SystemRoot%\Profiles\Administrator or profile of renamed Administrator account	Administrators SYSTEM	Full Control			
folder, subfolders, & files		Full Control			
12. %SystemRoot%\Profiles\All Users	Administrators	Full Control			
folder, subfolders, & file.	Authenticated Users	Read, Execute			
	SYSTEM	Full Control			
13. %SystemRoot%\Profiles\Default User	Administrators	Full Control			
folder, subfolders, & files	Authenticated Users	Read, Execute			
	SYSTEM	Full Control			
14. %SystemRoot%\Profiles\UserName\	Administrators	Full Control			
Desktop	Authenticated Users	Read, Execute			
Folder, subfolders, & files	CREATOR OWNER	Full Control			
	SYSTEM	Full Control			
15. %SystemRoot%\Profiles\UserName\Favorites	Administrators	Full Control			
folder, subfolders, & files	Authenticated Users	Read, Execute			
	CREATOR OWNER	Full Control			
	SYSTEM	Full Control			
16. %SystemRoot%\regedit.exe file	Administrators	Full Control			
	SYSTEM	Full Control			
17. %SystemRoot%\repair	Administrators	Full Control			
	SYSTEM	Full Control			
(folder, subfolders, & files)					
18. %SystemRoot%\Security	Administrators	Full Control			
	SYSTEM	Full Control			
(folder, subfolders, & files)					
19. %SystemRoot%\SendTo	Administrators	Full Control			
	Authenticated Users	Read, Write, Execute			
(folder, subfolders, & files)	CREATOR OWNER	Full Control			
	SYSTEM	Full Control			
20. %SystemRoot%\Temporary Internet Files	Administrators	Full Control			
	Authenticated Users	Read, Write, Execute			
(folder, subfolders, & files)	CREATOR OWNER	Full Control			
	SYSTEM	Full Control			
B. Ensure that permissions on critical binary files in the %SYSTEMDIRECTORY%					
1. %SystemDirectory%	Administrators	Full Control			
	Authenticated Users	Read, Execute			

		(folder, subfolders, & files)	CREATOR OWNER	Full Control			
			SYSTEM	Full Control			
		2. %SystemDirectory%\config	Administrators	Full Control			
			* SecAdmin	Change			
		(folder, subfolders, & files)	SYSTEM	Full Control			
			(* Group must first be created.)				
		3. %SystemDirectory%\Ntbackup.exe file	Administrators	Full Control			
			SYSTEM	Full Control			
		4. %SystemDirectory%\rcp.exe file	Administrators	Full Control			
			SYSTEM	Full Control			
		5. %SystemDirectory%\Rdisk.exe file	Administrators	Full Control			
			SYSTEM	Full Control			
		6. %SystemDrive%\msdos.sys *file*	Administrators	Full Control			
			SYSTEM	Full Control			
		7. %SystemDirectory%\repl\export	Administrators	Full Control			
			Authenticated Users	Read, Execute			
		(folder, subfolders, & files)	CREATOR OWNER	Full Control			
			Replicator	Read, Execute			
			SYSTEM	Full Control			
		8. %SystemDirectory%\repl\import	Administrators	Full Control			
			Authenticated Users	Read, Execute			
		(folder, subfolders, & files)	CREATOR OWNER	Full Control			
			Replicator	Modify			
			SYSTEM	Full Control			
		9. %SystemDirectory%\rexec.exe file	Administrators	Full Control			
			SYSTEM	Full Control			
		10. %SystemDirectory%\rsh.exe file	Administrators	Full Control			
			SYSTEM	Full Control			
		11. %SystemDirectory%\spool\Printers	Administrators	Full Control			
			Authenticated Users	Modify			
		(folder, subfolders, & files)	CREATOR OWNER	Full Control			
			Replicator	Modify			
			SYSTEM	Full Control			
		C. Ensure that permissions on the file containing FTI are correctly set.					

AC-5	User rights assigned to users are commensurate with routine job responsibilities.	Procedures: 1. Click on Start button and select Programs | Administrative Tool | User Manager (or User Manager for Domain) from the menu. 2. Select Policies | User Rights within the User Manager window. 3. Check Show Advance Rights box in the bottom of					
		User Rights	**Authorized User Groups**				
		1. Access this computer from network	Administrator, Authenticated User				
		2. Act as part of the operating system	None				
		3. Add workstations to the domain	None				
		4. Back up files and directories	Administrators, Backup Operators				
		5. Bypass traverse checking	Authenticated Users				
		6. Change the system time	Administrators				
		7. Create a pagefile	Administrators				
		8. Create a token object	None				
		9. Create permanent shared object	None				
		10. Debug programs	None				
		11. Force shutdown from a remote system	Administrators				
		12. Generate security audits	None				
		13. Increase quotas	None				
		14. Increase scheduling priority	Administrators				
		15. Load and unload device drivers	Administrators				
		16. Lock pages in memory	None				
		17. Log on as a batch job	None				
		18. Log on as a service	None				
		19. Log on locally	Administrators, Backup Operators				
		20. Manage auditing and security log	Administrators				
		21. Modify firmware environment variables	Administrators				
		22. Profile single process	Administrators				
		23. Profile system performance	Administrators				
		24. Replace a process-level token	None				
		25. Restore files and directories	Administrators, Backup Operators				
		26. Shut down the system	Administrators				
		27. Take ownership of files or other objects	Administrators				

Registry Checks	**1. Go to Start, Run, type cmd or command** **2. Type reg.exe query <key>\<key>\<key> /v <Value>** **Example: reg.exe query hkcu\software\intel\indeo\4.1 /v EnabledAccessKey**

Security Policy	**1. Go to Start, Run, type cmd or command** **2. Type "gpresult /Z > C:\gpresult_output_<hostname>** **3. Copy file to external drive for later analysis**

IRS Safeguard SCSEM Legend

Test Case Tab: Execute the test cases and document the results to complete the IRS Safeguard Computer Security review. Reviewer is required to complete the following columns: Actual Results, Comments/Supporting Evidence.

Test ID	Identification number of SCSEM test case
NIST ID	NIST 800-53/PUB 1075 Control Identifier
Test Objective	Objective of test procedure.
Test Steps	Detailed test procedures to follow for test execution.
Expected Results	The expected outcome of the test step execution that would result in a Pass.
Actual Results	The actual outcome of the test step execution, i.e., the actual configuration setting observed.
Pass/Fail	Reviewer to indicate if the test case pass, failed or is not applicable.
Comments / Supporting Evidence	Reviewer to include any supporting evidence to confirm if the test case passed., failed on not applicable As evidence, provide the following information for the following assessment methods: 1. Interview - Name and title of the person providing information. Also provide the date when the information is provided. 2. Examination - Provide the name, title, and date of the document referenced as the evidence. Also provide section number where the pertinent information is resident within the document (if possible). Ensure all supporting evidence to verify the test case passed or failed. If the control is marked as NA, then provide appropriate justification as to why the control is considered NA.